PRODUKTHANDBUCH

WebShield-Gerät

VERSION 2.5

A Network Associates Business

COPYRIGHT
© 2001–2002 Networks Associates Technology, Inc. Alle Rechte vorbehalten. Diese Veröffentlichung darf in keiner Form und in keiner Weise ohne die schriftliche Genehmigung von Network Associates Technology, Inc., oder ihren Lieferanten und angeschlossenen Unternehmen ganz oder teilweise reproduziert, übertragen, in einem Abrufsystem gespeichert oder in eine andere Sprache übersetzt werden. Diese Genehmigung können Sie schriftlich bei der Rechtsabteilung von Network Associates unter der folgenden Adresse beantragen: 3965 Freedom Circle, Santa Clara, California 95054, USA, oder rufen Sie unter (+1) -972-308-9960 an.

MARKEN
Active Security, ActiveHelp, ActiveShield, AntiVirus Anyware (und Design), Bomb Shelter, Building a World of Trust, Certified Network Expert, Clean-Up, CleanUp Wizard, Cloaking, CNX, CNX Certification Certified Network Expert (und Design), CyberCop, CyberMedia, CyberMedia UnInstaller, Data Security Letter (und Design), Design (Logo), Design (Hase mit Hut), Design (stilisiertes N), Disk Minder, Distributed Sniffer System, Distributed Sniffer System (in Katakana), Dr Solomon's, Dr Solomon's Label, Enterprise SecureCast, EZ SetUp, First Aid, ForceField, Gauntlet, GMT, GroupShield, Guard Dog, HelpDesk, HomeGuard, Hunter, I C Expert, ISDN TEL/SCOPE, LAN Administration Architecture (und Design), LANGuru, LANGuru (in Katakana), LANWords, Leading Help Desk Technology, LM1, M (und Design), Magic Solutions, Magic University, MagicSpy, MagicTree, MagicWord, McAfee Associates, McAfee, McAfee (in Katakana), McAfee (und Design), NetStalker, MoneyMagic, More Power To You, MultiMedia Cloaking, myCIO.com, myCIO.com design (CIO Design), myCIO.com Your Chief Internet Officer & Design, NAI & Design, Net Tools, Net Tools (in Katakana), NetCrypto, NetOctopus, NetRoom, NetScan, NetShield, NetStalker, Network Associates, Network General, Network Uptime!, NetXray, NotesGuard, Nuts & Bolts, Oil Change, PC Medic, PC Medic 97, PCNotary, PGP, PGP (Pretty Good Privacy), PocketScope, PowerLogin, PowerTelNet, Pretty Good Privacy, PrimeSupport, Recoverkey, Recoverkey – International, Registry Wizard, ReportMagic, RingFence, Router PM, SalesMagic, SecureCast, Service Level Manager, ServiceMagic, SmartDesk, Sniffer, Sniffer (in Hangul), SniffMaster, SniffMaster (in Hangul), SniffMaster (in Katakana), SniffNet, Stalker, Stalker (stilisiert), Statistical Information Retrieval (SIR), SupportMagic, TeleSniffer, TIS, TMACH, TMEG, TNV, TVD, TNS, TSD, Total Network Security, Total Network Visibility, Total Service Desk, Total Virus Defense, Trusted MACH, Trusted Mail, UnInstaller, Virex, Virus Forum, ViruScan, VirusScan, VShield, WebScan, WebShield, WebSniffer, WebStalker, WebWall, Who's Watching Your Network, WinGauge, Your E-Business Defender, ZAC 2000 und Zip Manager sind eingetragene Marken von Network Associates, Inc. und/oder ihren angeschlossenen Unternehmen in den USA oder anderen Ländern. Alle weiteren in diesem Dokument aufgeführten Marken sind geschützte Marken ihrer jeweiligen Inhaber.

LIZENZVERTRAG
HINWEIS FÜR ALLE BENUTZER: LESEN SIE DEN ENTSPRECHENDEN RECHTLICHEN VERTRAG FÜR DIE VON IHNEN ERWORBENE LIZENZ SORGFÄLTIG DURCH. ER ENTHÄLT DIE ALLGEMEINEN BESTIMMUNGEN UND BEDINGUNGEN FÜR DIE VERWENDUNG DER LIZENZIERTEN SOFTWARE. WENN SIE NICHT WISSEN, WELCHEN LIZENZTYP SIE ERWORBEN HABEN, LESEN SIE DIE LIEFERDOKUMENTE UND ALLE WEITEREN LIZENZ- ODER BESTELLUNTERLAGEN, DIE DER SOFTWARE BEILIEGEN ODER DIE SIE ALS TEIL DES ERWORBENEN PRODUKTS ERHALTEN HABEN (EINE BROSCHÜRE, EINE DATEI AUF DER PRODUKT-CD ODER EINE DATEI AUF DER WEBSITE, VON DER SIE DAS SOFTWAREPAKET HERUNTERGELADEN HABEN). WENN SIE NICHT MIT ALLEN BESTIMMUNGEN DES VERTRAGS EINVERSTANDEN SIND, DÜRFEN SIE DIE SOFTWARE NICHT INSTALLIEREN. IST DIES DER FALL, KÖNNEN SIE DAS PRODUKT GEGEN RÜCKERSTATTUNG DES KAUFPREISES AN NETWORKS ASSOCIATES ODER AN IHREN HÄNDLER ZURÜCKGEBEN.

Inhaltsverzeichnis

Vorwort vii
Funktion vii
Zielgruppe vii
Weitere Informationen vii
Kontaktaufnahme mit McAfee und Network Associates vii

Kapitel 1. Einführung 9
Funktionsweise des Geräts 10
Verwendungsweise des Geräts 13
Proxy- oder Transparenzmodus? 13
SMTP-Szenarios 15
FTP-Szenarios 24
HTTP-Szenarios 28
POP3-Szenarios 30
Verwenden mehrerer Geräte zur Verbesserung Ihrer Konfiguration . . 33
Fail-Over, Fail-Closed und Fail-Open 34
Fail-Over 35
Fail-Closed 36
Fail-Open 36

Kapitel 2. Proxies 39
Einführung 39
Verwalten der Protokolle 39

Kapitel 3. E-Mail (SMTP) 41
Einführung 41
Funktionen 41
Virenscan 42
Einrichten eines Postmasters 42
Inhaltsüberwachung 43

Anti-Relay 43
Erlauben und Verweigern von Relay 43
Sperraktion 44
Anti-Spam 44
Erlauben und Verweigern von Spam 44
Schwarze Listen 44
Routing-Zeichen 45
Sperraktion 45
Umgang mit Anlagen 45
Gründe für die Kontrolle einer Anlage 45
Konfiguration 46
Allgemeine Konfigurationseinstellungen 46
Hinzufügen von Erläuterungen 47
Gründe für Erläuterungen 47

Kapitel 4. FTP (File Transfer Protocol) 49
Einführung 49
Konfiguration 49
FTP im ASCII-Modus 50

Kapitel 5. Surfen im Internet (HTTP) 51
Einführung 51
Konfiguration 52

Kapitel 6. E-Mail-Download (POP3) 53
Einführung 53
Generischer Proxy 53
Dedizierter Proxy 53
Konfiguration 54
Allgemeine Konfigurationseinstellungen 54

Kapitel 7. Virenscan 55
Einführung 55
Die heuristische Analyse 55
Sicherheitsstufen 56
Handhabung infizierter Nachrichten 56

Automatische Aktualisierung 57
Antiviren-Software 57
Gründe für Updates 57
Bester Zeitpunkt für Updates 58
Planen von Updates 58

Kapitel 8. Inhaltsüberwachung 59
Einführung 59
Beispiele für Regeln 59
Vertraulicher Umgang mit Informationen 60
Verringern der Netzwerkbelastung 61
Abblocken beleidigender Wörter 61
Abblocken belästigender E-Mails 61
Verringern von Ablenkungen 62
Erstellen von Regeln 62
Festlegen einer Bezeichnung für eine Regel 63
Festlegen eines Anwendungsbereichs der Regel 63
Festlegen der auszuführenden Aktion bei Auslösung der Regel 63
Festlegen des Wortes oder Ausdrucks, das/der erkannt werden soll .64
Optionale fortgeschrittene Funktionen 65
Kontext 65
Nähe 65

Kapitel 9. Warnungen 67
Einführung 67
Informationsverteilung 67
Festlegen von Details 68
Überwachen kritischer Stufen 68
Umgang mit E-Mail-Problemen 68

Kapitel 10. Berichte und Diagramme 69
Einführung 69
Informationen im Protokoll 69
Drilldown bei den Informationen durchführen 70
CSV-Format 71

Kapitel 11. Wartung des Geräts 73

Einführung 73
Konfiguration 74
Hostname des Geräts 74
Domäne 75
Netzwerkadressen 75
Protokolle 76
E-Mail (SMTP) 77
Dateiübertragung (FTP) 79
Mail-Download (POP3) 79

Anhang A. Standardeinstellungen 81

Systemeinstellungen 81
E-Mail-Einstellungen (SMTP) 83
Einstellungen für Dateiübertragung (FTP) 85
Einstellungen für das Surfen im Internet (HTTP) 85
Einstellungen für Mail-Download (POP3) 86
Einstellungen für die Virenprüfung 87
Einstellungen für Protokolle und Warnungen 88

Index 89

Vorwort

Funktion

In diesem Produkthandbuch wird die Software des WebShield-Geräts vorgestellt, und es werden die Eigenschaften und Funktionen des Produkts erläutert.

Informationen zur Installation finden Sie im Installationshandbuch. Informationen zur Konfiguration finden Sie in der Online-Hilfe.

Zielgruppe

Dieses Handbuch wurde für System- und Netzwerkadministratoren geschrieben, die für die Betreuung des Antiviren-Programms in ihrem Unternehmen verantwortlich sind.

Weitere Informationen

In den Versionshinweisen sind alle anderen im Lieferumfang des Geräts enthaltenen Dokumente aufgelistet. Verwenden Sie diese Dokumente, um das Gerät optimal zu nutzen und es den Anforderungen Ihres Unternehmens anzupassen.

Kontaktaufnahme mit McAfee und Network Associates

Im Online-Hilfesystem finden Sie eine Verknüpfung zu Kontaktinformationen mit folgendem Inhalt:

- Eine Liste mit Telefonnummern, Anschriften, Webadressen und Faxnummern der Network Associates-Niederlassungen in den Vereinigten Staaten von Amerika und weltweit.
- Kontaktinformationen für Dienstleistungen und Ressourcen.

Einführung 1

Bei dem hier vorgestellten Gerät handelt es sich um einen speziell angefertigten Server, der Ihr Netzwerk vor Computerviren und unerwünschten Inhalten schützt. Es ist komplett über einen Web-Browser konfigurierbar und kann in fast allen Netzwerkumgebungen eingesetzt werden. Bei einwandfreier Installation und Konfiguration scannt das Gerät folgenden Datenverkehr:

- Simple Mail Transfer Protocol (SMTP) E-Mail-Nachrichten
- File Transfer Protocol (FTP)-Austausch
- HTTP (Hypertext Transfer Protocol) für das Surfen im Internet
- Post Office Protocol Version 3 (POP3) Internet E-Mail-Nachrichten

Im vorliegenden Handbuch werden die Gerätefunktionen beschrieben. Sie können nun überlegen, wie Sie es am besten in Ihrem Netzwerk einsetzen. Die einzelnen Funktionen werden detailliert in den nachfolgenden Kapiteln beschrieben.

Informationen zur Installation des Geräts erhalten Sie im Installationshandbuch.

Informationen zur Konfiguration und Wartung des Geräts entnehmen Sie der Online-Hilfe.

Die Software des Geräts verfügt über die folgenden Funktionen:

- Sie arbeitet im Proxy- oder Transparenzmodus (siehe Seite 13).
- Sie scannt E-Mail-Anhänge nach Viren und anderen schädlichen Elementen und säubert und löscht infizierte Dateien (einschließlich komprimierter Dateien und Makros) bzw. stellt sie unter Quarantäne.
- E-Mails werden nach unerwünschten oder brisanten Inhalten gescannt.
- Unerwünschte E-Mails (*Spam*) werden abgeblockt.
- Der Zugriff auf unerwünschte Websites wird gesperrt.
- Weiterleitung an Dritte wird verhindert.
- Die Anzahl und die Größe von E-Mail-Anhängen wird kontrolliert.
- Alle Geräteaktivitäten werden protokolliert und umfassende Berichte und Diagramme erstellt.

- Die Antiviren-Software wird automatisch aktualisiert und Schutz vor neuen Viren gewährleistet.
- Warnungen vor Viren- und Spam-Angriffen werden umgehend ausgegeben.

Funktionsweise des Geräts

Das WebShield-Gerät bietet Proxies für SMTP-, FTP-, HTTP- und POP3-Protokolle. Es teilt seine Ressourcen zwischen den Proxies auf, wobei der eingehende und ausgehende Datenverkehr jedes Protokolls auf Viren geprüft wird (Abbildung 1-1). Standardmäßig sind alle Proxies aktiviert, und die Virenprüfung wird in jede Richtung erzwungen.

HINWEIS: Das Gerät scannt Mail-Downloads (POP3), ohne die Richtung zu ermitteln (siehe „POP3-Szenarios“ auf Seite 30).

Das Gerät verfügt über eine Liste interner Netzwerke, mit deren Hilfe es erkennen kann, ob durchgehender Verkehr aus einer internen oder einer externen Quelle stammt (also eingehend oder ausgehend ist). Wenn Sie das Gerät konfigurieren, müssen Sie die internen Netzwerke und Domänen innerhalb der Firewall Ihres Unternehmens dieser Liste hinzufügen, ansonsten werden diese standardmäßig als externe Netzwerke und Domänen interpretiert.

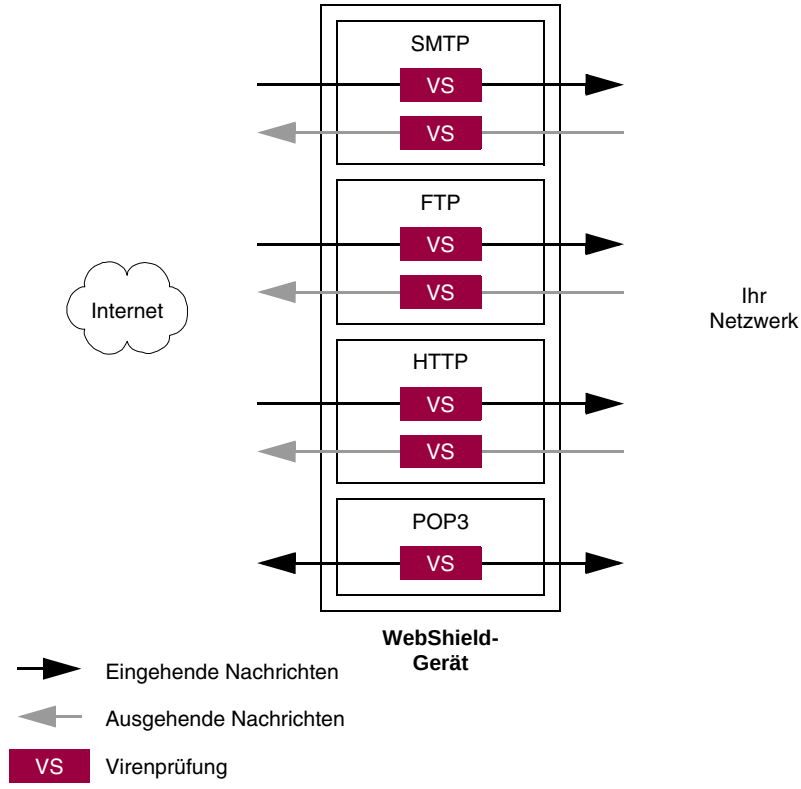


Abbildung 1-1. Virenprüfung eingehenden und ausgehenden Verkehrs

Das Aktivieren und Deaktivieren der Proxies und der Virenprüfung ist in zwei Ebenen aufgeteilt. Dadurch wird höchste Flexibilität und Kontrolle sichergestellt, wenn Ihre Geräte ordnungsgemäß konfiguriert sind, die Protokolle durch das Gerät zu leiten.

Proxysteuerung

Jeder Proxy kann aktiviert oder deaktiviert werden. Falls Sie einen Proxy deaktivieren, kann der Datenverkehr dieses Protokolls das Gerät nicht passieren, so daß das Protokoll wirksam blockiert ist (Abbildung 1-2).

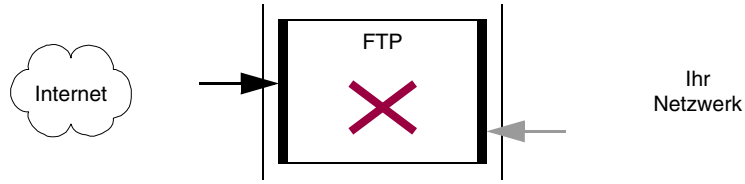


Abbildung 1-2. FTP-Proxy deaktiviert

Das Gerät bietet keine Ressourcen für einen deaktivierten Proxy, da für dieses Protokoll kein Datenverkehr gescannt werden muß.

Virenprüfung der Protokolle

Bei jedem Protokoll wird eingehender und ausgehender Datenverkehr getrennt auf Viren geprüft, mit Ausnahme von POP3, das zwischen eingehendem und ausgehendem Datenverkehr keinen Unterschied macht. Falls Sie die Virenprüfung für eine der beiden Richtungen deaktivieren, wird der Datenverkehr in dieser Richtung ungescannt durch das Gerät geleitet (Abbildung 1-3).

WICHTIG: Deaktivieren Sie die Virenprüfung nicht für aktivierte Protokolle, *es sei denn*, deren Datenverkehr wird an einem anderen Punkt im Netzwerk gescannt. Wenn Sie zulassen, daß nicht überprüfter Datenverkehr in Ihr Unternehmen gelangt und es verläßt, öffnen Sie eine Sicherheitslücke für Viren.

Konfigurieren Sie Ihre anderen Netzwerkgeräte so, daß sie die Protokolle durch das Gerät leiten, so daß nichts das Gerät umgehen kann.

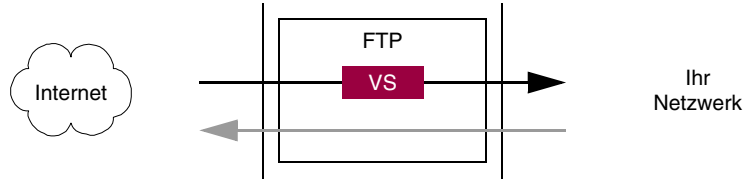


Abbildung 1-3. Ausgehende FTP-Virenprüfung deaktiviert

Verwendungsweise des Geräts

Sie können das Gerät in nahezu jeder Netzwerktopologie verwenden. Es ist äußerst flexibel und kann im Proxy- oder Transparenzmodus eingesetzt werden, wodurch Sie es den Anforderungen Ihres Unternehmens anpassen können.

Da die möglichen Topologiekombinationen zu zahlreich sind, um sie alle zu erwähnen, werden in diesem Abschnitt einige Szenarios für die Protokolle vorgestellt, um zu demonstrieren, wie Sie das Gerät in Ihr vorhandenes Netzwerk integrieren können. Wenn Sie in bezug auf die Topologie Ihres Netzwerks unsicher sind und nicht wissen, wie Sie das Gerät integrieren sollen, wenden Sie sich an Ihren Netzwerkfachmann.

Fail-Over-, Fail-Closed- und Fail-Open-Szenarios (siehe Seite 34).

WICHTIG: Um ein bestimmtes Protokoll zu scannen, müssen Sie im allgemeinen Ihre anderen Netzwerkgeräte oder Clientcomputer so konfigurieren, daß das Protokoll durch das Gerät geleitet wird, so daß nichts das Gerät umgehen kann.

Aus Sicherheitsgründen wird empfohlen, daß Sie das Gerät *innerhalb* Ihres Unternehmens und *hinter* einer ordnungsgemäß konfigurierten Firewall betreiben.

Proxy- oder Transparenzmodus?

Das Gerät kann in zwei verschiedenen Modi eingesetzt werden:

- **Proxymodus** (wird auch *expliziter Proxy* genannt)
- **Transparenzmodus** (wird auch *transparenter Proxy* genannt)

HINWEIS: Das Gerät kann immer nur einen dieser Modi anwenden. Die Entscheidung für den passenden Modus ist von Bedeutung (hängt meist von der Ausstattung und der Topologie des Netzwerks ab), denn der Modus hat Auswirkungen auf die physischen Verbindungen und die Verwaltungseinstellungen, die am Gerät vorgenommen werden müssen.

Version 2.0 und 2.1 des WebShield-Geräts verfügten nur über den Proxymodus. Der Transparenzmodus wurde in Version 2.5 eingeführt.

Proxymodus

Im Proxymodus (expliziter Proxy) ist das Gerät mit dem Netzwerk verbunden und überwacht den eingehenden Datenverkehr (über den Port LAN1). In diesem Fall müssen Sie Ihre Clients und allen anderen Geräte so konfigurieren, daß sie den SMTP-, FTP-, HTTP- und POP3-Datenverkehr an das WebShield-Gerät senden. Dieses scannt den Datenverkehr gemäß Ihren Einstellungen und leitet ihn dann an das nächste Gerät weiter (diesen Vorgang nennt man *Proxying*).

Am WebShield-Gerät selbst kann der Proxymodus rasch konfiguriert werden, das Konfigurieren Ihrer anderen Geräte (für das Senden des Datenverkehrs an das WebShield-Gerät) hingegen erschwert in manchen Netzwerken die Implementierung. Dieser Modus eignet sich beispielsweise für Netzwerke, deren Clients und andere Geräte über ein einzelnes Gerät (beispielsweise einen Web-Cache) eine Verbindung zur Firewall herstellen. In diesem Fall müssen nur die Verbindungsinformationen für den Web-Cache und die Firewall geändert werden (zur Kommunikation über das WebShield-Gerät).

Transparenzmodus

Im Transparenzmodus (transparenter Proxy) klinkt sich das WebShield-Gerät physisch in das Netzwerk ein (über die Anschlüsse LAN1 und LAN2) und empfängt somit den gesamten eingehenden Datenverkehr. Es scannt den SMTP-, FTP-, HTTP- und POP3-Datenverkehr gemäß Ihren Einstellungen (ignoriert anderen Datenverkehr) und leitet die Daten dann weiter. In dieser Konfiguration arbeitet das Gerät wie ein Router, indem es sich unsichtbar in den Datenstrom einklinkt (es wird *transparent*).

Der Transparenzmodus eignet sich für Netzwerke, deren Clients und andere Geräte direkt mit der Firewall verbunden sind, da in diesem Fall nicht alle Geräte konfiguriert werden müssen, um den Datenverkehr an das WebShield-Gerät weiterzuleiten. Sie müssen nur die Routing-Informationen für das WebShield-Gerät konfigurieren und einige Routing-Informationen für die Geräte auf beiden Seiten des WebShield-Geräts ändern (die an die Ports LAN1 und LAN2 angeschlossen sind).

Wenn Sie den Transparenzmodus verwenden, können Sie die erforderlichen Routing-Informationen konfigurieren. Sie können statische Routen angeben oder dynamisches Routing verwenden, um die Routing-Informationen abzuhören, die von den Routern in Ihrem Netzwerk gesendet werden. Wenn Sie das dynamische Routing verwenden, können Sie auch die Systemdiagnoseseite des WebShield-Geräts verwenden, um dessen Routing-Tabelle anzuzeigen und sicherzustellen, daß es die Routing-Informationen erhält.

SMTP-Szenarios

In diesem Abschnitt werden die folgenden, üblichen SMTP-Topologien vorgestellt:

- Ein Standort (siehe Seite 15).
- Ein Standort mit direktionalem Scannen (siehe Seite 17).
- Zwei Standorte (siehe Seite 20).
- Entmilitarisierte Zone (DMZ, siehe Seite 22).
- Internationales Unternehmen (siehe Seite 23).

Topologie 1: Ein Standort

Diese Topologie (Abbildung 1-4 oder Abbildung 1-5) kommt häufig in kleinen Firmen mit wenigen hundert Benutzern zum Einsatz.

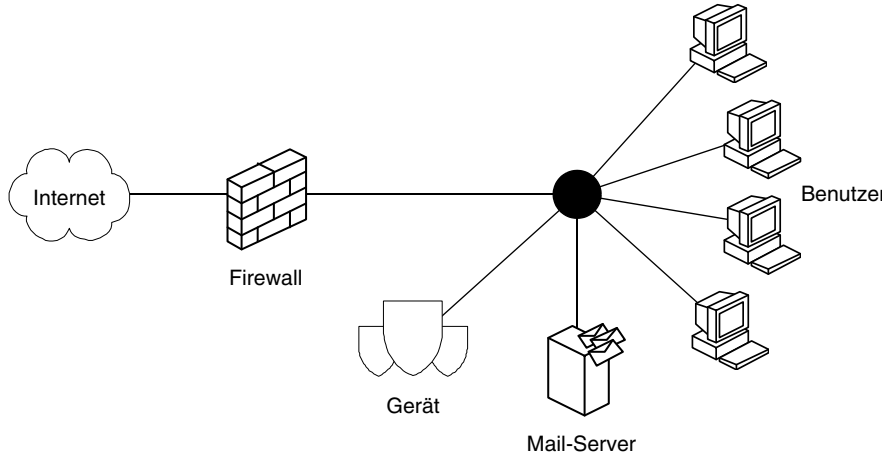


Abbildung 1-4. Ein Standort: Proxymodell

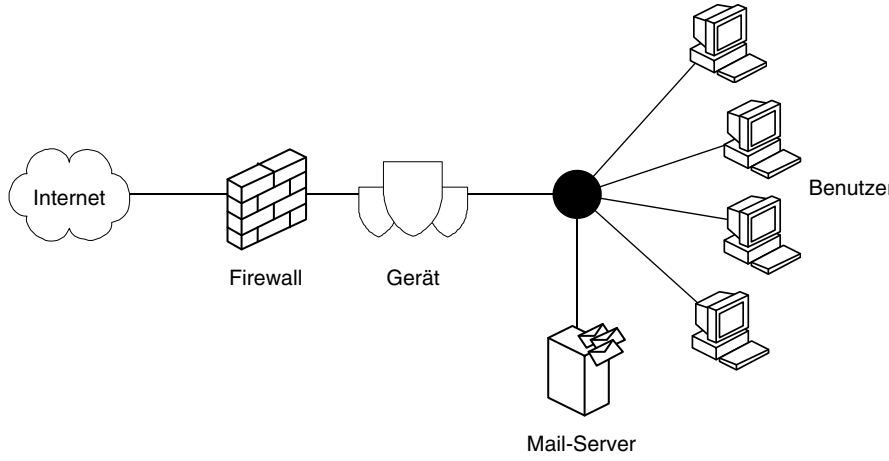


Abbildung 1-5. Ein Standort: Transparenzmodell

WICHTIG: Bei dieser Konfiguration müssen Sie sicherstellen, daß Benutzer ausgehende Nachrichten nicht direkt an die Firewall oder das Gerät senden können. Dies kann mit einer Firewall-Richtlinie durchgesetzt werden.

Die Konfiguration hat folgende Auswirkungen:

- Aus dem Internet empfangene SMTP-E-Mail-Nachrichten dürfen in das Unternehmen gelangen. Nachrichten, die wieder ins Internet zurückgeleitet werden sollen, werden abgewiesen.
- SMTP-E-Mail-Nachrichten, die das Gerät passieren, dürfen das Unternehmen verlassen. Alle anderen Meldungen aus dem lokalen Netzwerk werden abgewiesen.

Konfigurieren Sie die Firewall, das Gerät und den Mail-Server, um eingehende und ausgehende Nachrichten wie in Abbildung 1-6 gezeigt weiterzuleiten.

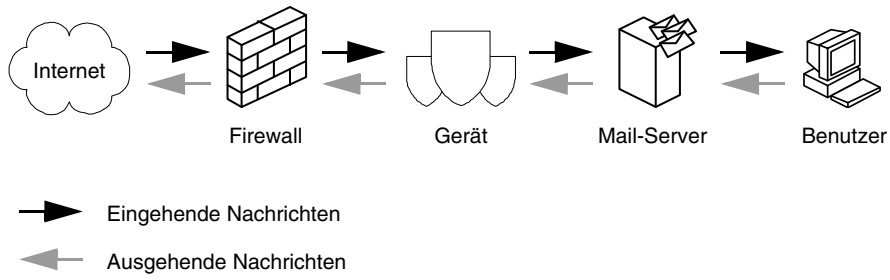


Abbildung 1-6. Ein Standort: Strom von E-Mail-Nachrichten

Dies ist eine *ausfallsichere* Konfiguration: Falls die Netzwerkverbindung des Geräts ausfällt, bleiben die ausgehenden Nachrichten auf dem Mail-Server und die eingehenden Nachrichten bleiben an oder außerhalb der Firewall. Dadurch wird sichergestellt, daß ungescannte E-Mail-Nachrichten nicht in Ihr Mail-System gelangen oder dieses verlassen können.

Topologie 2: Ein Standort mit direktionalem Scannen

Diese Topologie (Abbildung 1-7 und Abbildung 1-8 auf Seite 18) ist eine Verbesserung der Ein-Standort-Topologie (Seite 15). Sie beinhaltet ein zweites Gerät. Das erste Gerät ist zum Scannen eingehender Daten bestimmt, das zweite zum Scannen ausgehender Daten.

Durch die Verwendung von zwei Geräten wird der Durchsatz beim Scannen verdoppelt.

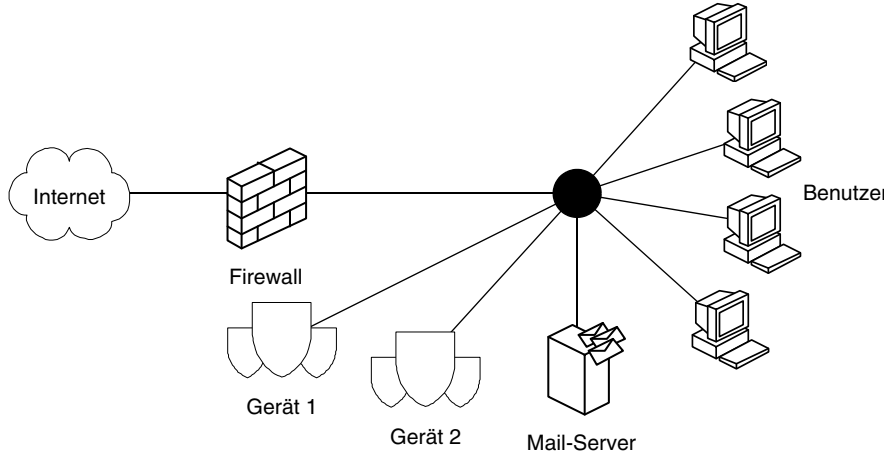


Abbildung 1-7. Ein Standort mit direktionalem Scannen: Proxymodell

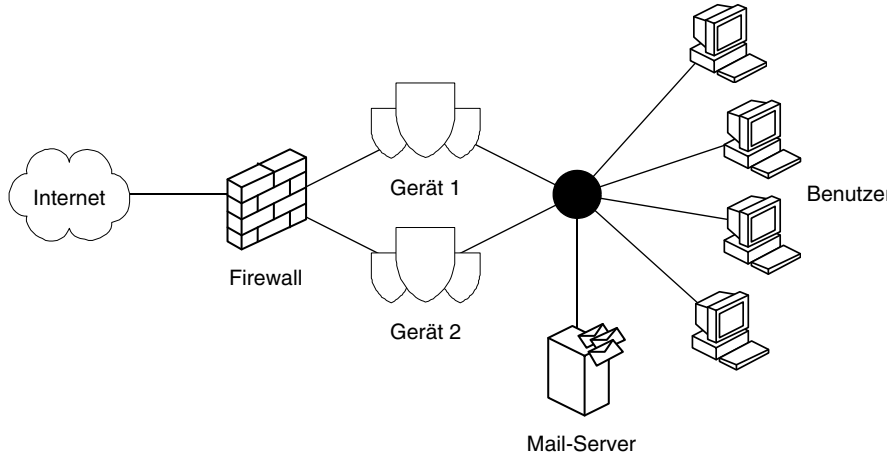


Abbildung 1-8. Ein Standort mit direktionalem Scannen: Transparenzmodell

WICHTIG: Bei dieser Konfiguration müssen Sie sicherstellen, daß Benutzer ausgehende Nachrichten nicht direkt an die Firewall oder das Gerät senden können. Dies kann mit einer Firewall-Richtlinie durchgesetzt werden.

Die Konfiguration hat folgende Auswirkungen:

- Aus dem Internet empfangene SMTP-E-Mail-Nachrichten dürfen in das Unternehmen gelangen. Nachrichten, die wieder ins Internet zurückgeleitet werden sollen, werden abgewiesen.
- SMTP-E-Mail-Nachrichten, die das Gerät passieren, dürfen das Unternehmen verlassen. Alle anderen Meldungen aus dem lokalen Netzwerk werden abgewiesen.

Konfigurieren Sie die Firewall, die Geräte und Mail-Server, um eingehende und ausgehende Nachrichten wie in Abbildung 1-9 gezeigt weiterzuleiten.

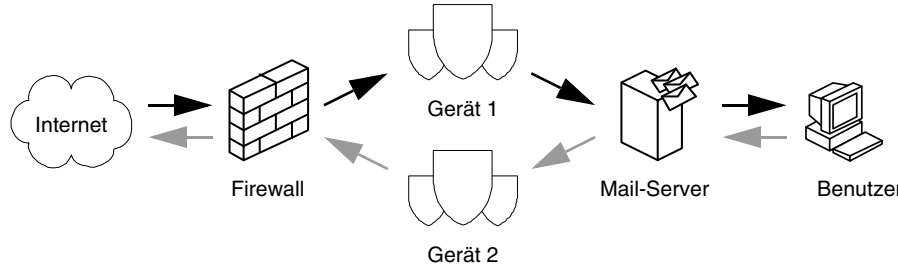


Abbildung 1-9. Ein Standort mit direktionalem Scannen: Strom von E-Mail-Nachrichten

Dies ist eine *direktionale ausfallsichere* Konfiguration: beide Geräte arbeiten unabhängig voneinander, wie im folgenden dargestellt:

- Falls die Netzwerkverbindung des ersten Geräts ausfällt, bleiben die eingehenden Daten an oder außerhalb der Firewall. Dadurch wird sichergestellt, daß ungescannte E-Mail-Nachrichten nicht in Ihr Mail-System gelangen können. Das Scannen ausgehender Daten bleibt unbeeinflußt.
- Falls die Netzwerkverbindung des zweiten Geräts ausfällt, bleiben die ausgehenden Daten auf den Mail-Servern. Dadurch wird sichergestellt, daß ungescannte E-Mail-Nachrichten Ihr Mail-System nicht verlassen können. Das Scannen eingehender Daten bleibt unbeeinflußt.

Dadurch wird die Möglichkeit größeren Durchsatzes und größerer Zuverlässigkeit geboten.

Topologie 3: Mehrere Standorte

Diese Topologie (Abbildung 1-10) ist für Firmen üblich, bei denen mehrere Standorte über ein WAN (Wide Area Network) miteinander verbunden sind. Jeder Standort hat einen Mail-Server, der die E-Mail-Nachrichten des Standorts verarbeitet, doch nur der Hauptstandort hat eine Verbindung zum Internet.

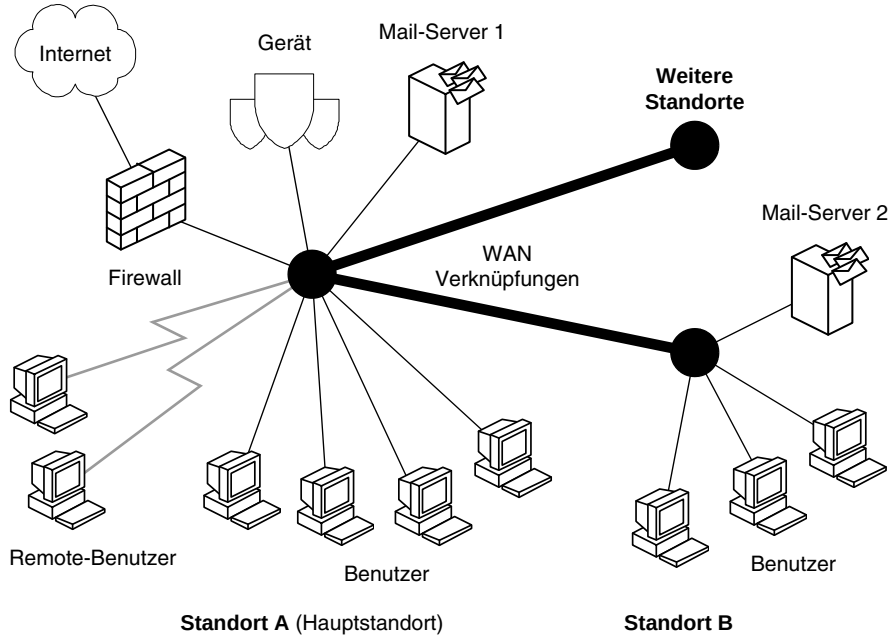


Abbildung 1-10. Mehrere Standorte: Proxymodell

Konfigurieren Sie die Firewall, das Gerät und die Mail-Server, um eingehende und ausgehende Nachrichten wie in Abbildung 1-11 gezeigt weiterzuleiten.

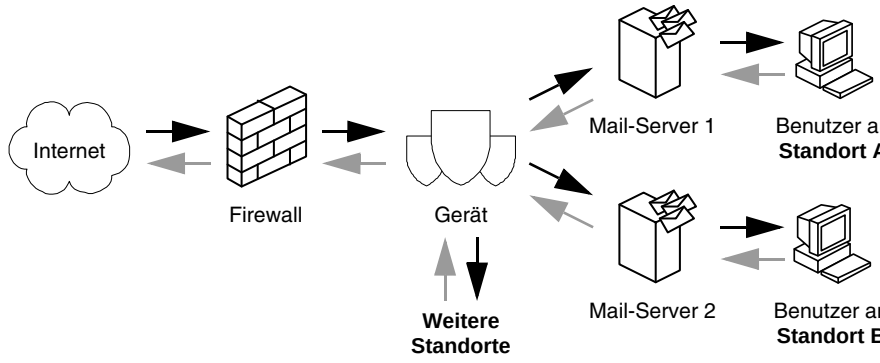


Abbildung 1-11. Mehrere Standorte: Strom von E-Mail-Nachrichten

Dies ist eine *ausfallsichere* Konfiguration, durch die sichergestellt wird, daß ungescannte E-Mail-Nachrichten nicht in Ihr Mail-System gelangen oder dieses verlassen können, falls die Netzwerkverbindung des Geräts ausfällt. Sie können ein zweites Gerät anschließen (siehe Seite 17), um den Durchsatz von Mails zu verdoppeln und eine *direktionale ausfallsichere* Konfiguration zu erstellen (Abbildung 1-12). Beide Geräte arbeiten unabhängig voneinander, entweder zum Scannen von eingehenden oder von ausgehenden Daten.

Konfigurieren Sie für eine direktionale ausfallsichere Konfiguration die Firewall, die Geräte und Mail-Server, um eingehende und ausgehende Nachrichten wie in Abbildung 1-12 gezeigt weiterzuleiten. Dadurch wird die Möglichkeit größeren Durchsatzes und größerer Zuverlässigkeit geboten.

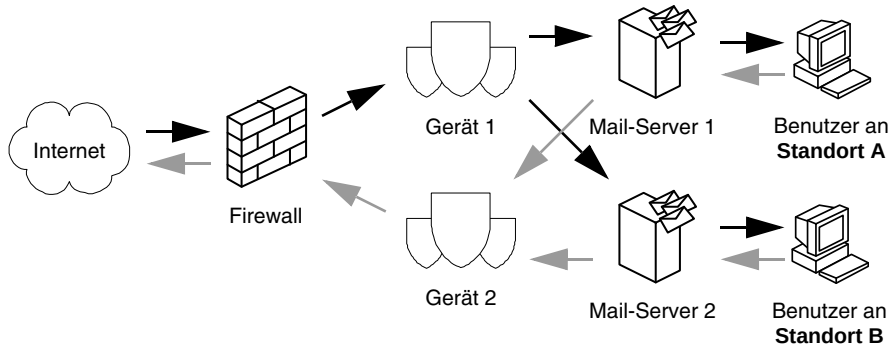


Abbildung 1-12. Mehrere Standorte mit direktionalem Scannen: Strom von E-Mail-Nachrichten

Topologie 4: Entmilitarisierte Zone (DMZ)

Diese Topologie (Abbildung 1-13) bietet eine höhere Sicherheit, doch die Konfiguration der Firewall ist recht umfassend, so daß sie für unerfahrene Benutzer nicht empfohlen wird. Die Topologie eignet sich für große Unternehmen mit einem DMZ-Sicherheitsmodell.

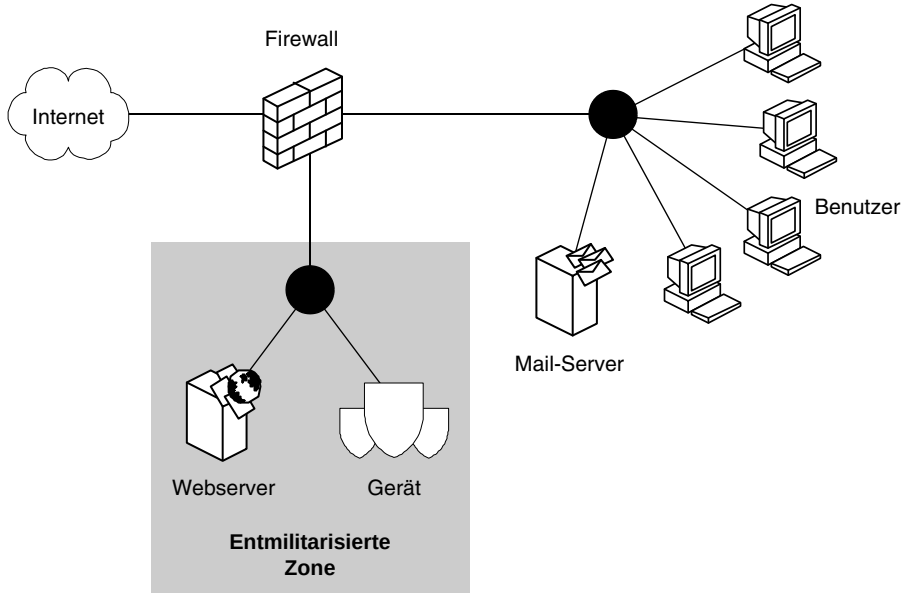


Abbildung 1-13. Entmilitarisierte Zone: Proxymodell

Konfigurieren Sie die Firewall, das Gerät und den Mail-Server, um eingehende und ausgehende Nachrichten wie in Abbildung 1-14 gezeigt weiterzuleiten.

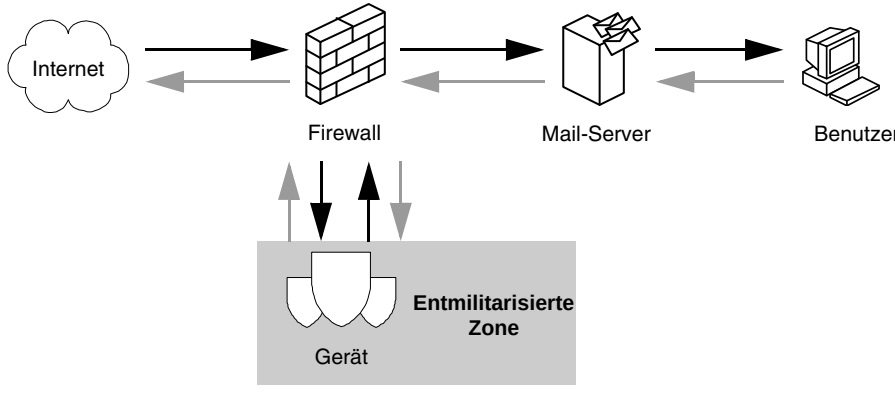


Abbildung 1-14. Entmilitarisierte Zone: Strom von E-Mail-Nachrichten

Die Firewall leitet die Nachrichten an das Gerät und vom Gerät weg, so daß jede Nachricht zweimal die Firewall passiert. Die Firewall ist konfiguriert, ausschließlich die E-Mail-Verbindungen von den Mail-Server-Relays zu akzeptieren.

Topologie 5: Internationale Unternehmen

Diese Topologie (Abbildung 1-15) umfaßt Netzwerke in verschiedenen Ländern, die über ein WAN (Wide Area Network) miteinander verbunden sind. Es gibt mehrere Geräte und mehrere Verbindungen, wodurch die Fehlertoleranz im Mail-Setup erhöht und sichergestellt wird, daß E-Mail-Nachrichten immer noch gescannt und gesendet werden können, wenn die Verbindung zu einem Gerät oder dem Internet ausfällt. Nachrichten für beliebige Netzwerkdomänen können über eine beliebige Internetverknüpfung empfangen werden. Der Haupt-Mail-Server (im folgenden Beispiel der Mail-Server *Berlin*) enthält das Hauptverzeichnis oder die Aliasliste für das gesamte Unternehmen und leitet die E-Mail-Nachrichten an die richtigen internen Mail-Server weiter.

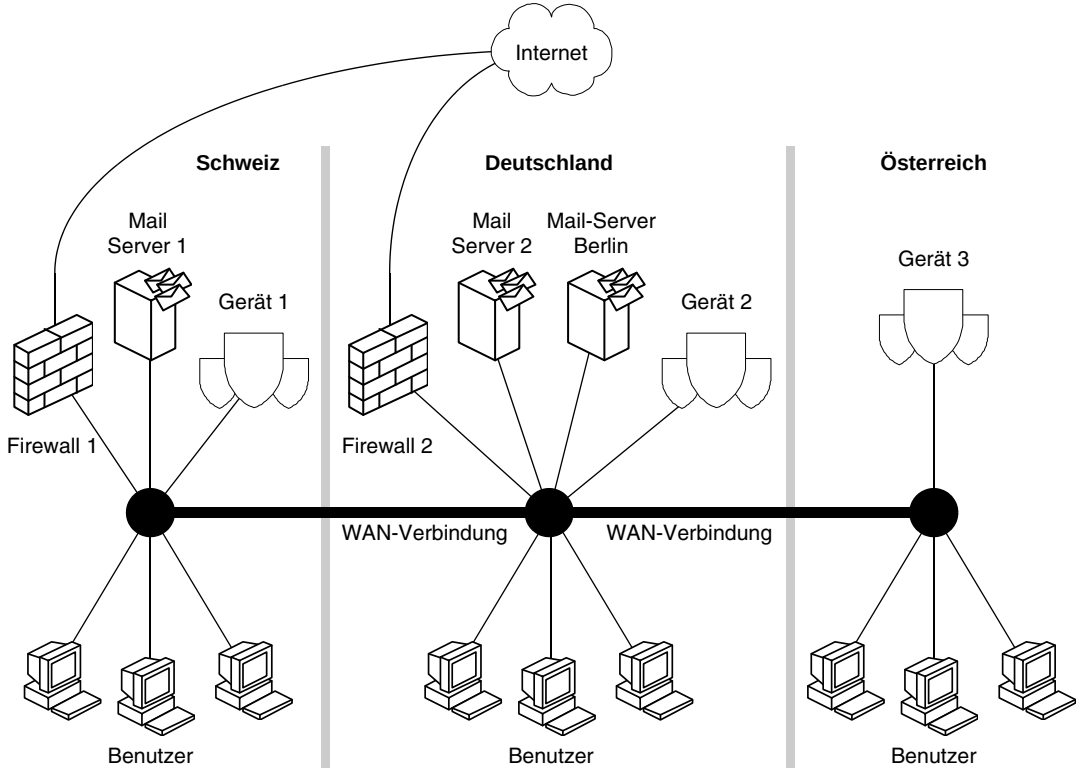


Abbildung 1-15. Internationale Unternehmen: Proxymodell

FTP-Szenarios

In diesem Abschnitt werden die folgenden FTP-Szenarios beschrieben:

- Ausgehende Kommunikation (siehe Seite 25).
- Eingehende Kommunikation, ein FTP-Server (Proxymodus) (siehe Seite 26).
- Eingehende Kommunikation, mehrere FTP-Server (Proxymodus) (siehe Seite 27).
- Ausgehende Kommunikation (Transparenzmodus) (siehe Seite 27).

> **TIP:** Es wird empfohlen, daß Sie Ihre eingehenden FTP-Informationen (an Ihren FTP-Server gesendete `put`-Befehle) mit dem Gerät schützen.

Für bidirektionales FTP-Scannen (eingehend und ausgehend) müssen Sie entweder echte FTP-Clients (Software wie beispielsweise CuteFTP) oder Befehlszeilen-FTP-Clients verwenden.

Einige Web-Browser wie Microsoft Internet Explorer enthalten einen FTP-Client (FTP-Software). Falls Sie versuchen, mit dieser Art von Client eine FTP-Verbindung herzustellen, wird die Kommunikation als HTTP-Aufruf über eine FTP-Verbindung gesendet. Das Gerät läßt keinen HTTP-Verkehr über den FTP-Proxy zu und blockiert die Kommunikation dementsprechend.

Um diese Art von Client weiter zu verwenden, konfigurieren Sie die FTP-Proxies Ihres Browsers auf denselben Port, den das Gerät für den HTTP-Proxy verwendet (standardmäßig Port 80). Beachten Sie, daß die FTP-über-HTTP-Funktion des HTTP-Proxy es lokalen Benutzern nicht ermöglicht, Dateien an externe Hosts zu übertragen. Solche Anfragen werden vom Gerät gelöscht.

Ausgehende Kommunikation

Abbildung 1-16 zeigt die Kommunikation, die erfolgt, wenn ein interner Benutzer auf einen internen FTP-Server (innerhalb des Unternehmens) oder auf einen externen FTP-Server (außerhalb des Unternehmens) zugreift.

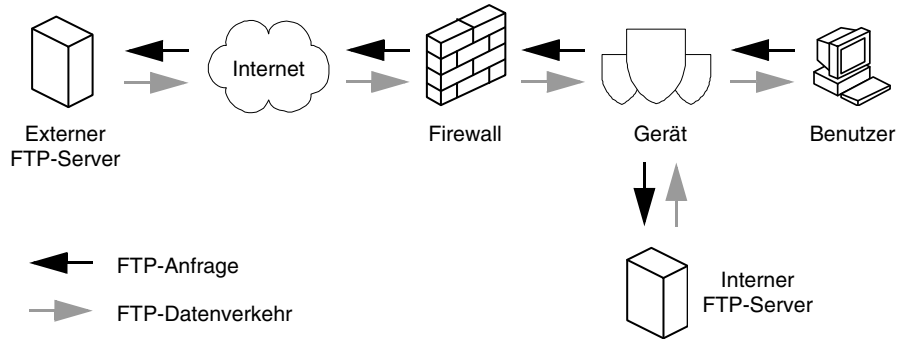


Abbildung 1-16. Ausgehende Kommunikation

Proxymodus

Im Proxymodus ist der FTP-Proxy des Geräts vom Typ „benutzer@host“: Benutzer müssen sowohl mit ihrem Benutzernamen als auch mit dem Hostnamen, getrennt durch das @-Symbol (beispielsweise `jan@ftp.meinefirma.com`) eine Verbindung zum FTP-Server herstellen.

❑ **HINWEIS:** Falls Ihre Firewall ebenfalls vom Typ „benutzer@host“ ist, können Sie den Übergabe-Host des Geräts als Firewall konfigurieren, so daß das Gerät (für den die Verbindung herstellenden Benutzer) wie die Firewall erscheint und reagiert. Das Gerät prüft FTP-Datenverkehr immer noch mit seinen Einstellungen für FTP-Scannen auf Viren.

Bei dieser Konfiguration müssen Sie den FTP-Client konfigurieren, das Gerät als Proxy-Server zu verwenden.

Transparenzmodus

Im Transparenzmodus müssen Sie die FTP-Clients nicht konfigurieren, wenn der Datenverkehr über das Gerät erfolgt.

Eingehende Kommunikation, ein FTP-Server (Proxymodus)

In Abbildung 1-17 wird die Kommunikation gezeigt, die erfolgt, wenn ein externer Benutzer auf einen internen FTP-Server zugreift.

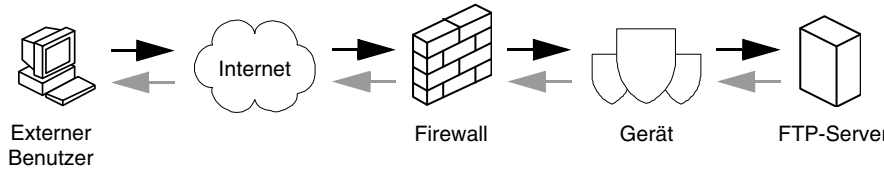


Abbildung 1-17. Eingehende Kommunikation: ein Server

Der FTP-Client des Benutzers wird von einem externen DNS-Server (im Internet) an die Firewall gesendet. Die Firewall leitet den gesamten Datenverkehr an das Gerät weiter, das diesen mit seinem Übergabe-Host an den FTP-Server weiterleitet. Sobald der Datenverkehr zurückkommt, wird dieser vom Gerät mit den *ausgehenden* FTP-Scan-Einstellungen auf Viren geprüft.

Die Kommunikation ist für den Benutzer transparent. Dessen FTP-Client meldet sich mit seinem Domänennamen (beispielsweise `ftp ftpserver.meinefirma.com`) beim FTP-Server an.

Bei dieser Konfiguration müssen Sie folgende Aktionen durchführen:

- Erstellen Sie Datensätze für den externen DNS-Server, so daß der FTP-Server mit der Firewall übereinstimmt.
- Konfigurieren Sie die Firewall nur zum Senden und Empfangen von internem FTP-Datenverkehr über das Gerät, so daß es nicht umgangen werden kann.
- Konfigurieren Sie das Gerät mit dem FTP-Server als eingehenden Übergabe-Host.

Eingehende Kommunikation, mehrere FTP-Server (Proxymodus)

Falls Ihr Unternehmen über mehrere FTP-Server verfügt, können Sie für jeden FTP-Server ein Gerät verwenden. Abbildung 1-18 zeigt die Kommunikation, die erfolgt, wenn ein externer Benutzer über die dedizierten Geräte auf die internen FTP-Server zugreift.

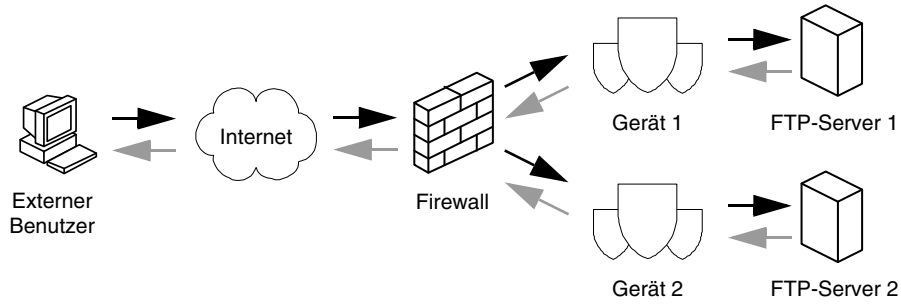


Abbildung 1-18. Eingehende Kommunikation: mehrere Server

Ein externer DNS-Server (im Internet) sendet den FTP-Client des Benutzers an die Firewall. Die Firewall leitet den gesamten Datenverkehr an das entsprechende Gerät weiter, das den Datenverkehr mit Hilfe seines Übergabe-Hosts an den FTP-Server weiterleitet. Sobald der Datenverkehr zurückkommt, wird dieser vom Gerät mit den *ausgehenden* FTP-Scan-Einstellungen auf Viren geprüft. Die Kommunikation ist für den Benutzer transparent. Dessen FTP-Client meldet sich mit seinem Domänennamen (beispielsweise `ftp ftpserver1.meinefirma.com`) beim FTP-Server an.

Bei dieser Konfiguration müssen Sie folgende Aktionen durchführen:

- Erstellen Sie Datensätze für den externen DNS-Server, so daß die FTP-Server mit der Firewall übereinstimmen.
- Konfigurieren Sie die Firewall nur zum Senden und Empfangen von internem FTP-Datenverkehr über das Gerät, so daß es nicht umgangen werden kann.
- Konfigurieren Sie jedes Gerät mit dem entsprechenden FTP-Server als eingehenden Übergabe-Host.

Ausgehende Kommunikation (Transparenzmodus)

Im Transparenzmodus müssen Sie die FTP-Server nicht konfigurieren, wenn der Datenverkehr über das Gerät erfolgt, denn die Benutzer stellen eine direkte Verbindung zu den FTP-Servern her.

HTTP-Szenarios

In diesem Abschnitt werden die folgenden HTTP-Szenarios beschrieben:

- Ausgehende Kommunikation (Proxymodus) (siehe unten).
- Eingehende Kommunikation (Proxymodus) (siehe Seite 29).
- Transparenzmodus (siehe Seite 30).

> **WICHTIG:** Das Gerät nimmt stellvertretend HTTP-Datenverkehr entgegen und scannt diesen (standardmäßig an Port 80).

Ausgehende Kommunikation (Proxymodus)

Abbildung 1-19 zeigt die Kommunikation, die erfolgt, wenn ein interner Benutzer auf einen externen Webserver zugreift.

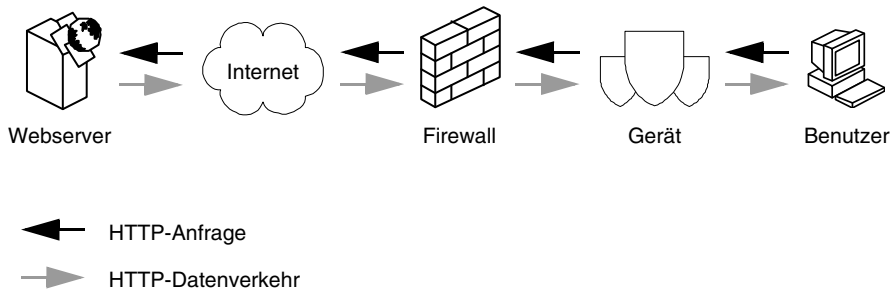


Abbildung 1-19. Ausgehende Kommunikation

Der HTTP-Client des Benutzers sendet eine Anfrage an den HTTP-Proxy des Geräts, der den Datenverkehr entweder stellvertretend mit seinem Übergabe-Host an die Firewall weiterleitet oder versucht, über die Standardroute eine Verbindung zum Webserver herzustellen. Sobald der Datenverkehr zurückkommt, wird dieser vom Gerät mit den *eingehenden* HTTP-Scan-Einstellungen auf Viren geprüft und anschließend an den Client weitergeleitet.

Die Kommunikation ist für den Benutzer transparent. Dessen HTTP-Client meldet sich mit seinem Domänennamen (beispielsweise `http://www.externefirma.com`) beim Webserver an.

Bei dieser Konfiguration müssen Sie folgende Aktionen durchführen:

- Konfigurieren Sie den HTTP-Client, das Gerät als Proxy-Server zu verwenden.

- Konfigurieren Sie die Firewall nur zum Senden und Empfangen von internem HTTP-Datenverkehr über das Gerät, so daß es nicht umgangen werden kann.

Sie können das Gerät mit der Firewall als ausgehenden Übergabe-Host konfigurieren. Falls Sie dies nicht tun, versucht das Gerät, über die Standardroute eine Verbindung zu externen Webservern herzustellen.

Eingehende Kommunikation (Proxymodus)

Abbildung 1-20 zeigt die Kommunikation, die erfolgt, wenn ein externer Benutzer auf einen internen Webserver zugreift.

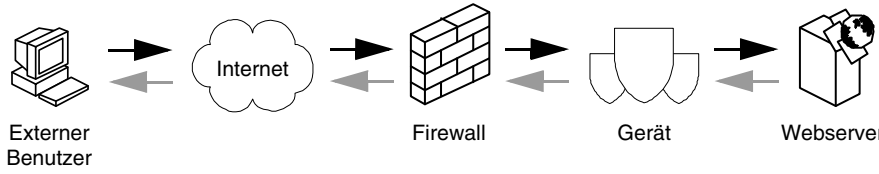


Abbildung 1-20. Eingehende Kommunikation

Der HTTP-Client des Benutzers wird von einem externen DNS-Server (im Internet) an die Firewall gesendet. Die Firewall leitet den gesamten Datenverkehr an das Gerät weiter, das einen internen DNS-Server (innerhalb des Unternehmens) nach der IP-Adresse für den internen Webserver abfragt und anschließend den Datenverkehr weiterleitet. Sobald der Datenverkehr zurückkommt, wird dieser vom Gerät mit den *ausgehenden* HTTP-Scan-Einstellungen auf Viren geprüft.

Die Kommunikation ist für den Benutzer transparent. Dessen HTTP-Client meldet sich mit seinem Domänennamen (beispielsweise `http://www.meinefirma.com`) beim Webserver an.

Bei dieser Konfiguration müssen Sie folgende Aktionen durchführen:

- Erstellen Sie Datensätze für den externen DNS-Server, so daß der Webserver mit der Firewall übereinstimmt.
- Konfigurieren Sie die Firewall nur zum Senden und Empfangen von internem HTTP-Datenverkehr über das Gerät, so daß es nicht umgangen werden kann.
- Konfigurieren Sie das Gerät mit dem Webserver als eingehenden Übergabe-Host.
- Erstellen Sie Datensätze für den internen DNS-Server, der für das Gerät konfiguriert wurde. In den Datensätzen muß der Domänenname des Webservers mit dessen IP-Adresse übereinstimmen.

Transparenzmodus

Im Transparenzmodus müssen Sie die HTTP-Server oder Clients nicht konfigurieren, wenn der Datenverkehr über das Gerät erfolgt, denn die Benutzer stellen eine direkte Verbindung zu den HTTP-Servern her.

POP3-Szenarios

In diesem Abschnitt werden die folgenden POP3-Szenarios beschrieben:

- Ausgehende Kommunikation (Proxymodus) (siehe unten).
- Eingehende Kommunikation, ein POP3-Server (Proxymodus) (siehe Seite 31).
- Eingehende Kommunikation, mehrere POP3-Server (Proxymodus) (siehe Seite 32).
- Transparenzmodus (siehe Seite 33).

> **HINWEIS:** Das Gerät scannt Mail-Downloads (POP3), ohne die Richtung zu ermitteln (eingehend oder ausgehend).
>
> Ist das Gerät entsprechend konfiguriert, kann das Gerät sowohl generische als auch dedizierte POP3-Verbindungen verarbeiten.

Ausgehende Kommunikation (Proxymodus)

Abbildung 1-21 zeigt die Kommunikation, die erfolgt, wenn ein interner Benutzer auf einen externen POP3-Server zugreift.

Der POP3-Client des Benutzers (POP3-E-Mail-Software) stellt eine Verbindung zum Gerät her und „springt“ dann über das Gerät auf den POP3-Server, indem er den für das Postfach erforderlichen Benutzernamen verwendet (beispielsweise `benutzername@pop3.externefirma.com`). Sobald der Datenverkehr zurückkommt, wird dieser vom Gerät mit den POP3-Scan-Einstellungen auf Viren geprüft.

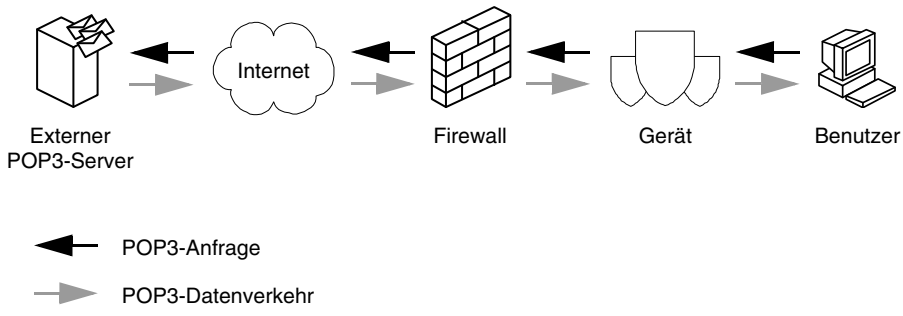


Abbildung 1-21. Ausgehende Kommunikation

Bei dieser Konfiguration müssen Sie den POP3-Client so konfigurieren, daß das Gerät als POP3-Server verwendet wird.

Eingehende Kommunikation, ein POP3-Server (Proxymodus)

Abbildung 1-22 zeigt die Kommunikation, die erfolgt, wenn ein externer Benutzer auf einen internen POP3-Server zugreift.

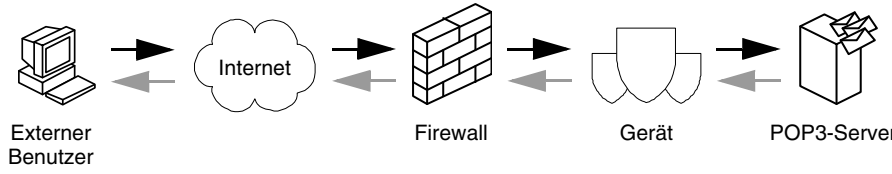


Abbildung 1-22. Eingehende Kommunikation: ein Server

Der POP3-Client des Benutzers wird von einem externen DNS-Server (im Internet) an die Firewall gesendet. Die Firewall leitet den gesamten Datenverkehr an das Gerät weiter, das den Verkehr mit seinen POP3-Scan-Einstellungen scannt. Danach leitet das Gerät den Datenverkehr über seine dedizierte Verbindung an den POP3-Server weiter. Sobald der Datenverkehr zurückkommt, wird dieser vom Gerät mit den POP3-Scan-Einstellungen auf Viren geprüft.

Die Kommunikation ist für den Benutzer transparent. Dessen POP3-Client stellt eine Verbindung zum entsprechenden Postfach auf dem POP3-Server her.

Bei dieser Konfiguration müssen Sie folgende Aktionen durchführen:

- Erstellen Sie Datensätze für den externen DNS-Server, so daß der POP3-Server mit der Firewall übereinstimmt.
- Konfigurieren Sie die Firewall nur zum Senden und Empfangen von internem POP3-Datenverkehr über das Gerät, so daß es nicht umgangen werden kann.
- Konfigurieren Sie das Gerät mit einer dedizierten Verbindung zum POP3-Server. Verwenden Sie dazu die Port-Nummer 110.

Eingehende Kommunikation, mehrere Server (Proxymodus)

Falls Ihr Unternehmen über mehrere POP3-Server verfügt, können Sie eine der folgenden Aktionen durchführen:

- Konfigurieren Sie das Gerät mit dedizierten Verbindungen für jeden POP3-Server.

  Dies erfordert für jeden POP3-Server einen unterschiedlichen Port, so daß externe Clients wissen müssen, welchen Port sie verwenden sollen. Unter Umständen müssen Sie diese Ports auch an Ihrer Firewall öffnen (aktivieren).

- Verwenden Sie für jeden POP3-Server ein Gerät (Abbildung 1-23 auf Seite 32).

  Dadurch bleibt die Kommunikation für den Benutzer transparent. Sie müssen Datensätze für den externen DNS-Server erstellen, so daß die POP3-Server mit der Firewall übereinstimmen.

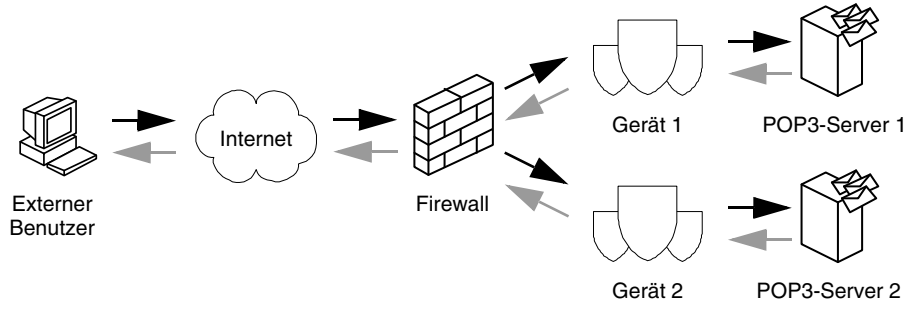


Abbildung 1-23. Eingehende Kommunikation: mehrere Server

Bei dieser Konfiguration müssen Sie folgende Aktionen durchführen:

- Erstellen Sie Datensätze für den externen DNS-Server, so daß die POP3-Server mit der Firewall übereinstimmen.
- Konfigurieren Sie die Firewall nur zum Senden und Empfangen von internem POP3-Datenverkehr über das Gerät, so daß es nicht umgangen werden kann.
- Konfigurieren Sie jedes Gerät mit einer dedizierten Verbindung zum entsprechenden POP3-Server. Verwenden Sie dazu die Port-Nummer 110.

Transparenzmodus

Im Transparenzmodus müssen Sie die POP3-Server oder Clients nicht konfigurieren, wenn der Datenverkehr über das Gerät erfolgt, denn die Benutzer stellen eine direkte Verbindung zu den POP3-Servern her.

Verwenden mehrerer Geräte zur Verbesserung Ihrer Konfiguration

Aus den vorangegangenen Szenarios ist zu ersehen, wie flexibel das Gerät bei der Verwendung in nahezu jeder Netzwerktopologie sein kann. Diese Flexibilität wird noch verbessert, wenn Sie wie nachfolgend erläutert mehrere Geräte zusammen verwenden:

- **Getrenntes Scannen von eingehendem und ausgehendem Datenverkehr**

  Sie können zwei Geräte verwenden, um das Scannen eingehender und ausgehender Daten unabhängig voneinander durchzuführen, wodurch eine *direktionale ausfallsichere* Konfiguration bereitgestellt wird. „Topologie 2: Ein Standort mit direktionalem Scannen“ auf Seite 17 zeigt ein Beispiel dafür.

- **Mehrere Geräte für bestimmte Protokolle**

  Falls Ihr Unternehmen sehr viel Datenverkehr für ein bestimmtes Protokoll empfängt, können Sie den verfügbaren Durchsatz beim Scannen erhöhen, indem Sie weitere Geräte hinzufügen. Anbieter von POP3-Postfächern beispielsweise können mehrere dedizierte Geräte zum Scannen von POP3 verwenden.

- **Fail-Over-Fehlertoleranz**

  Es kann Situationen geben, in denen der Datenverkehr Ihr Gerät nicht erreicht. Durch die Verwendung mehrerer Geräte können kontinuierliche Virenprüfung und kontinuierlicher Datenverkehr sichergestellt werden (siehe unten).

Fail-Over, Fail-Closed und Fail-Open

Es gibt Situationen, in denen Ihre Netzwerkgeräte keinen Datenverkehr an Ihr Gerät weiterleiten können. Es folgen einige Beispiele:

- Es liegen interne Netzwerkprobleme vor, beispielsweise ein langsames Netzwerk oder eine abgebrochene Verbindung.
- Der Datenverkehr ist sehr umfangreich und füllt vorübergehend die Puffer des Geräts.
- Das Gerät wurde abgeschaltet oder neu gestartet, möglicherweise, weil Sie dessen Software wiederherstellen oder die IP-Konfiguration ändern.

In diesem Fall müssen Sie entscheiden, wohin der für die Proxys des Geräts bestimmte Verkehr weitergeleitet werden soll. Folgende Konfigurationen können eingerichtet werden; alle erfordern entsprechende Änderungen in den Datensätzen Ihres DNS-Servers:

- Fail-Over (siehe Seite 35).
- Fail-Closed (siehe Seite 36).
- Fail-Open (siehe Seite 36).

Viele Personen verwenden die Ausdrücke *Fail-Over*, *Fail-Closed* und *Fail-Open*, um sich auf sehr unterschiedliche Konfigurationen zu beziehen. Aus diesem Grund enthält jedes Szenario in diesem Abschnitt eine kurze Beschreibung, in der die Art der Konfiguration beschrieben wird, auf die Bezug genommen wird.

HINWEIS: Dies betrifft nur den Datenverkehr, den das Gerät stellvertretend entgegennimmt. Der andere Datenverkehr wird normal durch Ihr Netzwerk geleitet.

Weitere Informationen zur Modifikation der DNS-Server-Software entnehmen Sie der Dokumentation des DNS-Servers.

Fail-Over

Eine Fail-Over-Konfiguration umfaßt zwei oder mehr Geräte, die eine Fehlertoleranz bieten. Falls das erste Gerät nicht erreicht werden kann, wird der Datenverkehr an das zweite Gerät weitergeleitet, das dann stellvertretend den Datenverkehr entgegennimmt und scannt (Abbildung 1-24).

Diese Konfiguration wird empfohlen, falls Sie mehrere Geräte haben. Dadurch werden kontinuierliche Virenprüfung und kontinuierlicher Datenverkehr sichergestellt, so daß jederzeit saubere Daten in Ihr Unternehmen gelangen und dieses verlassen können.

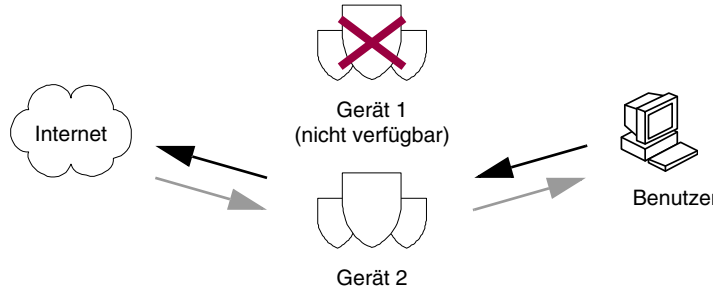


Abbildung 1-24. Fail-Over

TIP: Mit der Sicherungs- und Wiederherstellungsfunktion des Geräts können Sie das zweite Gerät schnell mit einer Konfiguration versehen, die der des ersten Geräts ähnelt. Speichern Sie dazu die Einstellungen der ersten Datei in einem Satz Konfigurationsdateien und stellen Sie die Dateien anschließend auf dem zweiten Gerät wieder her. Beachten Sie, daß Sie den Hostnamen und die IP-Adressen für das zweite Gerät ändern müssen, um einen Netzwerkkonflikt zu vermeiden.

Informationen zum Sichern und Wiederherstellen der Geräteeinstellungen finden Sie im Installationshandbuch.

Bei dieser Konfiguration müssen Sie die MX (Mail Exchange)-Datensätze Ihres DNS-Servers wie folgt ändern:

- Fügen Sie das erste Gerät hinzu und geben Sie diesem höchste Priorität, so daß es den Datenverkehr als erstes empfängt.
- Fügen Sie das zweite Gerät hinzu und geben Sie diesem eine niedrigere Priorität, so daß es den Datenverkehr empfängt, wenn das erste Gerät nicht erreicht werden kann.
- Entfernen Sie die Datensätze für Ihre Server und anderen Geräte (*außer* Ihrer Firewall), so daß die Geräte nicht umgangen werden können.

Zum Fail-Over von FTP, HTTP und POP3 sind zusätzliche Geräte erforderlich, um ein automatisches Fail-Over zu gewährleisten.

Fail-Closed

Bei einer Fail-Closed-Konfiguration (auch *ausfallsicher* genannt) wird sichergestellt, daß kein Datenverkehr in Ihr Unternehmen gelangen bzw. dieses verlassen kann, wenn das Gerät nicht erreichbar ist (Abbildung 1-25).

Abbildung 1-25. Fail-Closed

Diese Art der Konfiguration wird empfohlen, wenn Sie nur ein Gerät haben, das den Virenschutz Ihres Unternehmens gewährleistet.

Bei dieser Konfiguration müssen Sie die Datensätze Ihres DNS-Servers wie folgt ändern:

- Fügen Sie das erste Gerät hinzu, so daß es Datenverkehr empfängt.
- Entfernen Sie die Datensätze für Ihre Server und anderen Geräte (*außer* Ihrer Firewall), so daß die Geräte nicht umgangen werden können.

Fail-Open

Bei einer Fail-Open-Konfiguration wird sichergestellt, daß Datenverkehr in Ihr Unternehmen gelangen und dieses verlassen kann, wenn das Gerät nicht erreichbar ist (Abbildung 1-26).

Abbildung 1-26. Fail-Open

WICHTIG: Diese Art der Konfiguration wird nicht empfohlen, da infiziertes Material ungescannt in Ihr Unternehmen gelangen und dieses verlassen kann. Fügen Sie nach Möglichkeit weitere Geräte hinzu, um eine Fail-Over-Konfiguration zu bilden. Auf diese Weise wird der Datenverkehr zunächst an diese Geräte weitergeleitet, *bevor* er ungescannt passiert.

Stellen Sie sicher, daß Ihre Mail-Server, Dateiserver, Clients (Benutzer) und weiteren Geräte durch Antiviren-Software von McAfee geschützt sind.

Bei dieser Konfiguration müssen Sie die Datensätze Ihres DNS-Servers wie folgt ändern:

- Fügen Sie die Geräte hinzu und geben Sie diesen höchste Priorität, so daß sie den Datenverkehr als erstes empfangen.
- Fügen Sie Ihre Server, die Firewall und weitere Geräte hinzu, und geben Sie diesen niedrigere Prioritäten, so daß sie den Datenverkehr empfangen, wenn die Geräte nicht erreicht werden können.

Proxies 2

Einführung

Das Gerät schützt Ihr Netzwerk vor unerwünschten Inhalten und Computerviren in Dateien, die in Ihr Netzwerk gelangen und es verlassen. Es führt mehrere Software-Prozesse (oder *Proxies*) aus, die Daten verarbeiten, die in verschiedenen Protokollen empfangen wurden.

Damit mit den Protokollen gearbeitet werden kann, die Ihre Site verwenden möchte, muß das Gerät so konfiguriert sein, daß jeder Proxy effektiv funktionieren kann. Die jeweiligen Funktionen der einzelnen Protokolle werden in den entsprechenden Abschnitten beschrieben.

- SMTP – im allgemeinen als E-Mail bekannt (siehe Seite 41).
- FTP – im allgemeinen als Dateiübertragung oder *Herunterladen* bekannt (siehe Seite 49).
- HTTP – im allgemeinen als Webzugriff oder Browsing bekannt (siehe Seite 51).
- POP3 – im allgemeinen als E-Mail-Download bekannt (siehe Seite 53).

Verwalten der Protokolle

Für jeden Proxy sind einige Einstellungen erforderlich. Sie müssen beispielsweise eine Port-Nummer festlegen und bestimmen, ob ein Virenscan sowohl bei eingehendem als auch bei ausgehendem Verkehr erforderlich ist.

Alle Proxies haben ähnliche Einstellungen, die sich darauf auswirken, wie viele Ressourcen für die Handhabung des Protokolls aufgewendet werden. Die Einstellungen für die Anzahl der Listener, Verbindungen und Speicherzuweisungen werden in den jeweiligen Abschnitten detailliert beschrieben. Mit dem Gerät ist diese Konfiguration einfach. Wenn Sie das Gerät zum erstenmal verwenden, sind einige Standardwerte eingestellt. Sie können diese Einstellungen jederzeit wiederherstellen, wenn die modifizierten Werte unbrauchbar sind.

Das Gerät bietet eine weitere einfache Methode zum Einstellen dieser Werte. Sie können aus einer begrenzten Reihe typischer Verwendungszwecke wählen und es dem Gerät erlauben, die Einstellungen anzuwenden. Beispiel: Sie können eine hohe, niedrige oder mittlere Verwendung von SMTP-E-Mails auswählen.

E-Mail (SMTP) 3

Einführung

E-Mail stellt in der heutigen Geschäftswelt ein wichtiges Hilfsmittel dar. Der Austausch von E-Mails ist oftmals der ausschlaggebende Grund für Unternehmen, eine Verbindung zum Internet zur Verfügung zu stellen. Eine Internetverbindung ist jedoch nicht völlig ohne Risiko.

Der SMTP-Proxy scannt jede eingehende und ausgehende E-Mail nach Viren und analysiert den Inhalt anhand textbasierter Regeln.

Funktionen

Beim Transfer von E-Mails zwischen den internen und den externen Netzwerken führt das Gerät folgendes durch:

- Nachrichten und Anlagen werden nach Viren gescannt (siehe „Virenscan“ auf Seite 42).
- Nachrichten und Anlagen werden nach gesperrtem Inhalt gescannt (siehe „Inhaltsüberwachung“ auf Seite 43).
- Es wird verhindert, daß nicht autorisierte Benutzer Nachrichten über Ihre Site weiterleiten (siehe „Anti-Relay“ auf Seite 43).
- Unerwünschte Massen-E-Mails (auch *Spam* genannt) werden verhindert (siehe „Anti-Spam“ auf Seite 44).
- Die Anzahl der Anlagen wird kontrolliert (siehe „Umgang mit Anlagen“ auf Seite 45).
- Erläuterungen werden hinzugefügt (siehe „Hinzufügen von Erläuterungen“ auf Seite 47).

Virenscan

Eine E-Mail enthält unter Umständen Anlagen, beispielsweise Word-Dokumente, Tabellen oder ein Spiel. Alle diese Anhänge können Viren enthalten. Das Gerät kann nach entsprechender Konfiguration auf unterschiedliche Weise reagieren:

- Das Gerät ersetzt die Anlage durch eine leere Datei. Obwohl der Name der Anlage weiterhin sichtbar ist, ist diese nun harmlos.
- Das Gerät ersetzt die Anlage durch eine einfache Textdatei, die eine Nachricht enthält. Die Nachricht kann entsprechend angepaßt werden, so daß sie beispielsweise den Namen des Virus enthält.

Die zuvor infizierte E-Mail kann dann auf eine der folgenden Arten weitergeleitet werden:

- Sie kann zum beabsichtigten Empfänger weitergeleitet werden.
- Sie kann zum Absender zurückgeschickt werden – entweder mit einer leeren E-Mail-Adresse (eine standardmäßige Benachrichtigungsform) oder mit der E-Mail-Adresse des Postmasters (siehe nächster Abschnitt).

Weitere Informationen hierzu finden Sie unter „Virenscan“ auf Seite 55.

Einrichten eines Postmasters

Das Gerät kann einen Administrator (oder *Postmaster*) bestimmen, der Anfragen von Absendern bezüglich E-Mail-Nachrichten bearbeitet, die aufgrund von Viren oder gesperrten Inhalten zurückgeschickt wurden.

Wählen Sie einen Benutzer, der die E-Mails regelmäßig liest. Beispiele:

- ThomasBerger@firma.com
- mail_master@meinefirma.de

Neben einzelnen Namen können Sie Verteilerlisten, beispielsweise IT_Manager@firma.com, verwenden. In E-Mail-Programmen, beispielsweise Microsoft Outlook, können Ihre Empfänger ebenfalls Regeln verwenden, um ihre E-Mails weiterzuleiten, für den Fall, daß sie nicht verfügbar sind. Auf diese Weise können Sie sicher sein, daß Benutzerprobleme schnell angegangen werden.

Inhaltsüberwachung

Das Gerät kann den Inhalt von E-Mails scannen. Sie können Regeln erstellen, die Wörter und Ausdrücke angeben, die in E-Mails nicht erlaubt sind. Es können beliebig viele Regeln festgelegt werden, und bei jeder Regel können Wörter in unterschiedlichen Kombinationen angegeben werden. Beispiel: Sie können komplexe Regeln erstellen, bei denen die Verwendung eines Wortes in einer bestimmten Situation zulässig ist, aber in anderen Situationen nicht. Die Regeln sowie die Wörter und Ausdrücke, die sie enthalten, können schnell hinzugefügt, modifiziert oder gelöscht werden.

Einzelheiten hierzu finden Sie unter „Inhaltsüberwachung“ auf Seite 59.

Anti-Relay

Das Gerät verhindert das Weiterleiten an Dritte.

Das Weiterleiten von E-Mails wird häufig für böswillige Zwecke, beispielsweise *Mail-Bombing* oder *Spamming*, verwendet. Die Anti-Relay-Funktion verhindert, daß skrupellose Personen das Gerät oder die E-Mail-Server verwenden können, um E-Mails zu senden.

Stellen Sie sich einmal die möglichen Konsequenzen vor, wenn Ihre Geschäftspartner weitergeleitete Nachrichten (unter Umständen geschmackloser Art) erhalten, die offenbar von Ihrem Unternehmen stammen. Dank der Anti-Relay-Funktion können Sie solch peinliche Situationen verhindern und das professionelle Image Ihrer Firma wahren.

Die Anti-Relay-Funktion des Geräts verhindert das Weiterleiten von E-Mails (SMTP), die nicht von einer der Domänen stammen, die das Gerät akzeptiert. Sites, die alle Nachrichten weiterleiten, werden *offene Relays* genannt und zur Zeit als unerwünscht angesehen. Die Betreiber solcher Sites können von Organisationen, wie beispielsweise MAPS und ORBS, gesperrt werden, die die Verbreitung von Spam-Mail zu unterbinden versuchen.

Erlauben und Verweigern von Relay

Mit dem Gerät können Sie festlegen, welche Domänen Nachrichten weiterleiten dürfen (insbesondere lokale Domänen) und welche nicht. Sie können Domänen und Unterdomänen kombinieren, wenn Sie den Zugriff erteilen bzw. verweigern, um Ihre Netzwerkumgebung und Sicherheitsbedürfnisse wunschgemäß einzurichten.

Nachrichten mit speziellen Routing-Zeichen, wie beispielsweise „%“, können ebenfalls den Zugriff erlaubt oder verweigert bekommen.

Sperraktion

Nachdem das Gerät ermittelt hat, daß eine E-Mail *weitergeleitet* wurde, kann es auf zwei Arten damit umgehen. Das Gerät kann den Absender darüber informieren, daß die Nachricht abgelehnt wurde. Das Gerät kann dem Absender mitteilen, daß die Nachricht angenommen wurde, sie dann aber löschen. Die zweite Aktion wird allerdings nicht empfohlen, da dies zu weiteren Relays führen kann.

Anti-Spam

Das Gerät verhindert, daß Spam-Mails in Ihr Unternehmen gelangen.

Jegliche nicht angeforderten E-Mails können als Spam angesehen werden. Dazu gehören u. a. unerwünschte Werbe-E-Mails, das elektronische Pendant zu Reklame, oder spekulativen Werbeschriften. Es handelt sich dabei einfach um E-Mails, die Werbung enthalten und nicht vom Empfänger erwartet wurden. Solche E-Mails werden häufig in hundert- oder tausendfacher Ausführung gesendet. Wenn der Empfänger kein Kunde ist oder die Informationen nicht angefordert hat, ist die E-Mail normalerweise unerwünscht.

Häufig gestalten die *Verfasser von Spam-Nachrichten* die Betreffzeile der E-Mails so, daß der wahre Inhalt verborgen wird, und Beschwerden auf unschuldige Dritte zurückfallen. Andere Arten nicht angeforderter E-Mails werden ebenfalls als Spam angesehen, auch wenn sie nicht geschäftlicher Natur sind. Dazu können politische Nachrichten, Viruswarnungen, Virustäuschungen, Lyrik, Witze und Kettenbriefe zählen.

Erlauben und Verweigern von Spam

Sie können angeben, welche Domänen E-Mails senden oder nicht senden dürfen.

Schwarze Listen

Das Gerät kann so konfiguriert werden, daß es Listen mit bekannten Spam-Absendern berücksichtigt, so daß es deren Nachrichten entsprechend abblocken kann. Die Listen, die als „Real-time Black-Hole Lists“ (RBL) bekannt sind, werden von Organisationen, wie beispielsweise MAPS und ORBS, geführt.

Diese Listen enthalten Sites, die offenes Relay erlauben, und solche, die von Einwahlrechnern verwendet werden. Durch regelmäßiges Abrufen dieser Listen kann das Gerät die meisten Spam-Quellen abblocken.

Routing-Zeichen

Eine E-Mail-Adresse kann Routing-Zeichen enthalten (beispielsweise „%“ und „!“), die es ermöglichen, Nachrichten zwischen Computern weiterzugeben. Sie können diese Art von Relay abblocken, indem Sie angeben, welche Routing-Zeichen erlaubt bzw. nicht erlaubt werden.

Sperraktion

Nachdem das Gerät bestimmt hat, daß eine E-Mail Spam ist, kann es mit der Nachricht auf zwei Arten verfahren. Das Gerät kann den Absender darüber informieren, daß die Nachricht abgelehnt wurde. Das Gerät kann dem Absender mitteilen, daß die Nachricht angenommen wurde, sie dann aber löschen. Die zweite Aktion wird allerdings nicht empfohlen, da dies zu weiterem Spam führen kann.

Normalerweise verfährt das Gerät mit Spam unauffällig. Sie können jedoch einen Bericht auf Vorkommnisse von Spam-Mails anzeigen, damit Sie später die entsprechende Quelle untersuchen können.

Umgang mit Anlagen

Das Gerät kann die Verwendung von Anlagen bei E-Mails kontrollieren. Eine E-Mail besteht normalerweise aus zwei Komponenten:

- Nachrichtentext, der normalerweise kurz ist.
- Optional aus zusätzlichen Dateien, die an die Nachricht angehängt sind, beispielsweise Tabellen, Dokumente und Grafiken.

Gründe für die Kontrolle einer Anlage

Diese zusätzlichen Dateien können die Größe einer gesamten Nachricht erheblich erhöhen – eine normale Notiz, die nur ein paar Kilobyte groß wäre, kann dadurch auf mehrere Megabyte anwachsen. Normalerweise ist dieser Informationsfluß erforderlich, damit Ihr Unternehmen richtig funktioniert, aber es kann zu Problemen kommen, wenn Anlagen übermäßig verwendet werden oder gar Mißbrauch damit betrieben wird.

So werden beispielsweise häufig Computerspiele an E-Mails angehängt. Jedes Spiel kann einige Megabyte groß sein. Große Audio- oder Bilddateien – ob für private oder geschäftliche Zwecke – erreichen eine ähnliche Größe. Beliebte Dateien werden immer wieder kopiert und weitergeleitet und belasten Ihre Mail-Server, die dadurch für alle Benutzer spürbar langsamer werden.

Mit dem Gerät können Sie Anlagen von E-Mails unter Berücksichtigung der folgenden Aspekte abblocken:

- Größe der jeweiligen Anlage
- Anzahl der Anlagen
- Name der Anlage

  Dies ist nützlich für das Verhindern von Weiterleitungen beliebter Grafiken und Spiele. Spiele enthalten häufig Viren.

- Erweiterungsname

  Dadurch wird der Dateityp gekennzeichnet, beispielsweise Bilddateien oder Computerprogramme (EXE-Dateien). Diese letzte Funktion ermöglicht die Anwendung nützlicher Richtlinien im gesamten Unternehmen. Sie können die Verwendung großer Bitmap-Dateien (beispielsweise BMP) sperren, damit kompaktere Formate (beispielsweise GIF) verwendet werden. Doch Sie können nicht nur verhindern, daß Spiele weitergeleitet werden, sondern auch das illegale Kopieren von Software von Drittanbietern verringern. Der Fluß vertraulicher Informationen über die Firma (beispielsweise Datenbanken und Projektpläne) kann ebenfalls überwacht werden.

Konfiguration

Allgemeine Konfigurationseinstellungen

Wie auch bei den anderen Protokollen dieses Geräts können Sie die Einstellungen für dieses Protokoll aus einer Reihe typischer Situationen auswählen oder Sie können verschiedene Einstellungen genau Ihren Vorstellungen anpassen. Zu den Einstellungen gehören:

- Port-Nummer
- Anzahl der Listener.
  Das Gerät kann über eine beliebige Anzahl von Instanzen des Proxy verfügen, die den Verkehr empfangen. Wenn Sie diese Zahl erhöhen, steigern Sie somit die Anzahl der Transfers, die das Gerät gleichzeitig durchführen kann. Es gibt jedoch eine Grenze, bei der weitere Steigerungen die Leistung nicht mehr verbessern. Der Wert wird unter Umständen von anderen Proxy-Servern beeinflußt, die unterschiedliche Protokolle scannen, d. h. er ist von der gesamten Auslastung abhängig.

- Anzahl der Verbindungen pro Listener.
  Das Gerät kann über eine beliebige Anzahl gleichzeitiger Verbindungen für jede Instanz des Proxy verfügen. Jeder Proxy kann auch mehrere Verbindungen gleichzeitig handhaben. Dieser Wert entspricht der obengenannten Anzahl der Listener.

- Speichermenge pro Verbindung (für Virenscan zugewiesen).
  Das Gerät weist einen Speicherbereich für Virenscans zu. Wenn dieser Bereich überschritten wird, werden Mitteilungen auf der Festplatte gespeichert. Der Wert wird unter Umständen von anderen Proxy-Servern beeinflußt, die unterschiedliche Protokolle scannen, d. h. er ist von der gesamten Speicherverfügbarkeit abhängig.

Jede Einstellung verfügt über einen ursprünglichen Standardwert. Wenn Sie verschiedene neue Einstellungen ausprobieren, diese aber nicht zu optimalen Ergebnissen führen, können Sie die Standardwerte einfach wiederherstellen, da das Gerät sie beibehält.

Hinzufügen von Erläuterungen

Das Gerät ermöglicht es Ihnen, Erläuterungen an ein- und ausgehende E-Mails anzuhängen.

Eine Erläuterung ist ein Text (eine Erklärung, Informationen, ein rechtlicher Hinweis oder eine Warnung), den das Gerät an eine E-Mail anhängen kann, wenn diese es passiert.

Gründe für Erläuterungen

Indem Sie eine Erläuterung an ausgehende Nachrichten anhängen, können Sie die Haftbarkeit für Aussagen einschränken, die rechtliche Schäden verursachen könnten (beispielsweise beleidigende Bemerkungen). Erläuterungen sind ebenfalls nützlich für die Ablehnung von Nachrichtsinhalten als Ansicht des Unternehmens, um schädliche Publicity zu vermeiden. Beispielsweise:

> Die Informationen in dieser Nachricht sind vertraulich und nur für den Empfänger bestimmt. Wenn Sie diese Nachricht irrtümlich empfangen haben und Probleme vorliegen, benachrichtigen Sie den Absender bitte umgehend. Die nicht autorisierte Verwendung, Bekanntgabe, Kopie oder Änderung dieser Nachricht ist strengstens verboten.

Durch das Hinzufügen einer Erläuterung an eingehende Nachrichten können Sie Mitarbeiter darauf aufmerksam machen, daß alle E-Mails und Anlagen auf Viren und Inhalte gescannt werden.

FTP (File Transfer Protocol) 4

Einführung

Manchmal ist die einfachste Methode zum Übertragen von Daten von einem Computer auf einen anderen die Ausgabe einer Befehlszeile zum Übertragen der entsprechenden Dateien. Das File Transfer Protocol (FTP) ist eines von mehreren Protokollen, die dies ermöglichen. Das Gerät verfügt über einen FTP-Proxy, mit dem sichere Dateitransfers zwischen dem externen und dem internen Netzwerk ermöglicht werden.

Konfiguration

Wenn Dateien per FTP übertragen werden, werden alle Daten, die das Gerät passieren, nach Viren gescannt:

- Das Gerät führt Scans bei eingehendem FTP-Verkehr einschließlich aller Transfers, GET-Befehlen von internen Clients und PUT-Befehlen von externen Clients durch.
- Das Gerät führt Scans bei ausgehendem FTP-Verkehr, einschließlich aller GET-Befehle von internen Clients und PUT-Befehle von externen Clients durch.

Sie müssen bestimmen, ob der Virenscan sowohl bei ein- als auch ausgehendem Verkehr erforderlich ist. Werden andere Antiviren-Methoden auf Computern verwendet, die mit diesem verbunden sind, ist ein weiterer Virenscan unter Umständen nicht mehr nötig.

Wie auch bei den anderen Protokollen dieses Geräts können Sie die Einstellungen für dieses Protokoll aus einer Reihe typischer Situationen auswählen oder Sie können verschiedene Einstellungen genau Ihren Vorstellungen anpassen. Zu den Einstellungen gehören:

- Port-Nummer
- Anzahl der Listener.
  Das Gerät kann über eine beliebige Anzahl von Instanzen des Proxy verfügen, die den Verkehr empfangen. Wenn Sie diese Zahl erhöhen, steigern Sie somit die Anzahl der Transfers, die das Gerät gleichzeitig durchführen kann. Es gibt jedoch eine Grenze, bei der weitere Steigerungen die Leistung nicht mehr verbessern. Der Wert wird unter Umständen von anderen Proxy-Servern beeinflußt, die unterschiedliche Protokolle scannen, d. h. er ist von der gesamten Auslastung abhängig.

- Anzahl der Verbindungen pro Listener.
  Das Gerät kann über eine beliebige Anzahl gleichzeitiger Verbindungen für jede Instanz des Proxy verfügen. Jeder Proxy kann auch mehrere Verbindungen gleichzeitig handhaben. Dieser Wert entspricht der obengenannten Anzahl der Listener.

- Speichermenge pro Verbindung (für Virenscan zugewiesen).
  Das Gerät weist einen Speicherbereich für Virenscans zu. Wenn dieser Bereich überschritten wird, werden Mitteilungen auf der Festplatte gespeichert. Der Wert wird unter Umständen von anderen Proxy-Servern beeinflußt, die unterschiedliche Protokolle scannen, d. h. er ist von der gesamten Speicherverfügbarkeit abhängig.

Jede Einstellung verfügt über einen ursprünglichen Standardwert. Wenn Sie verschiedene neue Einstellungen ausprobieren, diese aber nicht zu optimalen Ergebnissen führen, können Sie die Standardwerte einfach wiederherstellen, da das Gerät sie beibehält.

FTP im ASCII-Modus

Dateien, die im ASCII-Modus übertragen werden, werden unter Umständen im Netzwerk in einem anderen Format gesendet, als es beim Ziel verwendet wird. Da der Virenscanner nicht feststellen kann, was das endgültige Format sein wird, werden Viren in binären Dateien, die im ASCII-Modus übertragen werden, möglicherweise nicht entdeckt.

Das Sperren von 8-Bit-Dateiübertragung im ASCII-Modus verhindert, daß binäre Dateien im ASCII-Modus übertragen werden. Allerdings kann dies auch dazu führen, daß einwandfreie Textdateien in 8-Bit-Zeichensätzen nicht übertragen werden. Wenn Ihre Benutzer Textdateien in 8-Bit-Zeichensätzen mittels FTP übertragen müssen, ist es am sichersten, die Dateien im binären Modus zu übertragen und sie mit Hilfe von Hilfsprogrammen, wie beispielsweise unix2dos bzw. dos2unix, in das entsprechende lokale Dateiformat zu konvertieren.

Surfen im Internet (HTTP) 5

Einführung

Mit Hilfe von Browsern und Webseiten ist es einfach, auf Informationen im Internet zuzugreifen. Wenn Benutzer über einen Browser auf das Internet zugreifen, stellt das Gerät mehrere Abwehrmechanismen zur Verfügung:

- Es werden alle Daten auf Programmviren gescannt.
- Das Gerät scannt Java-Klassen und Active X-Objekte, die als ausführbare Dateien angesehen werden und schädlichen Code ausführen könnten.
- Es werden optional Objekte gesperrt, die heruntergeladen werden können.

  Wenn eine Webseite angezeigt wird, lädt der Browser unter Umständen Active X-Komponenten, Java-Applets und Skript-Sprachen (beispielsweise Visual Basic oder Javascript) herunter. Der Virenscanner des Geräts entdeckt zwar schädliche Objekte, doch diese Funktion bietet zusätzliche Sicherheit.

- Das Gerät sperrt den Zugriff auf unerwünschte Websites.

  Das Internet bietet zwar eine Fülle von Informationen, doch einige Websites (beispielsweise über Sport, Reisen, Einkauf oder Unterhaltung) sind unter Umständen für Ihre Geschäftszwecke nicht erwünscht. Das Gerät kann den Zugriff auf bestimmte Websites sperren. Wenn ein Benutzer versucht, auf solche Sites zuzugreifen, wird ein Banner eingeblendet, das angibt, daß der Zugriff verweigert wird. Solch ein Zugriff wird ebenfalls vom Gerät aufgezeichnet und in Berichten vermerkt, die später untersucht werden können (siehe „Berichte und Diagramme“ auf Seite 69).

  Sie können den Zugriff auf eine Website sperren, indem Sie deren vollständige Adresse verwenden, beispielsweise *www.fussball.de*. Manchmal ist es jedoch effizienter, die Sperrung durch einen kurzen Namen anstatt eine vollständige Adresse durchzuführen. So kann man beispielsweise die ProSiebenSat1.Media AG sowohl unter der Webadresse *www.prosieben.com* als auch unter der URL *www.prosieben.net* erreichen. Wenn man den Zugriff auf diese Website also sperren wollte, müßte man am besten *prosieben* angeben.

Das Gerät verursacht keine Probleme bei einer Website-Filterung durch eine Firewall, die den HTTP-Verkehr überwacht. Fehlerberichte und Sperrmeldungen werden weiterhin generiert wie zu der Zeit, bevor das Gerät in Ihr Netzwerk implementiert wurde.

Konfiguration

Wie auch bei den anderen Protokollen dieses Geräts können Sie die Einstellungen für dieses Protokoll aus einer Reihe typischer Situationen auswählen oder Sie können verschiedene Einstellungen genau Ihren Vorstellungen anpassen. Zu den Einstellungen gehören:

- Port-Nummer
- Anzahl der Listener.
  Das Gerät kann über eine beliebige Anzahl von Instanzen des Proxy verfügen, die den Verkehr empfangen. Wenn Sie diese Zahl erhöhen, steigern Sie somit die Anzahl der Transfers, die das Gerät gleichzeitig durchführen kann. Es gibt jedoch eine Grenze, bei der weitere Steigerungen die Leistung nicht mehr verbessern. Der Wert wird unter Umständen von anderen Proxy-Servern beeinflußt, die unterschiedliche Protokolle scannen, d. h. er ist von der gesamten Auslastung abhängig.
- Anzahl der Verbindungen pro Listener.
  Das Gerät kann über eine beliebige Anzahl gleichzeitiger Verbindungen für jede Instanz des Proxy verfügen. Jeder Proxy kann auch mehrere Verbindungen gleichzeitig handhaben. Dieser Wert entspricht der obengenannten Anzahl der Listener.
- Speichermenge pro Verbindung (für Virenscan zugewiesen).
  Das Gerät weist einen Speicherbereich für Virenscans zu. Wenn dieser Bereich überschritten wird, werden Mitteilungen auf der Festplatte gespeichert. Der Wert wird unter Umständen von anderen Proxy-Servern beeinflußt, die unterschiedliche Protokolle scannen, d. h. er ist von der gesamten Speicherverfügbarkeit abhängig.

Jede Einstellung verfügt über einen ursprünglichen Standardwert. Wenn Sie verschiedene neue Einstellungen ausprobieren, diese aber nicht zu optimalen Ergebnissen führen, können Sie die Standardwerte einfach wiederherstellen, da das Gerät sie beibehält.

E-Mail-Download (POP3) 6

Einführung

POP3 (Post Office Protocol Version 3) ist ein E-Mail-Sammelprotokoll, mit dem E-Mails von einer Mailbox eines externen Servers heruntergeladen werden. Der Hotmail-Dienst von Microsoft ermöglicht Ihnen das Abrufen von E-Mail-Nachrichten mit Hilfe von POP3.

Es gibt zwei Betriebsmodi:

- Generischer Proxy – Ermöglicht eine Verbindung zu einem beliebigen POP3-Server. APOP (Authenticated POP) wird allerdings nicht unterstützt.
- Dedizierter Proxy – Ermöglicht Verbindungen zu dedizierten POP3-Servern mit APOP.

Generischer Proxy

Wenn über das Gerät eine Verbindung zu einem generischen Proxy hergestellt wird, trennt das Gerät den Benutzernamen, Hostnamen und die Port-Nummer durch die Begrenzungszeichen Raute (#) und Doppelpunkt (:). Benutzer#Host:Port

Sie können gegebenenfalls andere Begrenzungszeichen für das Gerät angeben.

Dedizierter Proxy

Wenn ein Benutzer über das Gerät eine Verbindung zu einem dedizierten Proxy herstellt, verwendet das Gerät einen festgelegten Port, um den POP3-Server zu erreichen. Sie müssen für jeden Server eine eindeutige Port-Nummer angeben. Es wird empfohlen, Zahlen zwischen 1024 und 32767 zu wählen, da die Zahlen bis 1024 in der Regel anderen Protokollen zugewiesen sind. Der Server verfügt über einen vollständigen Domänennamen (FQDN), beispielsweise pop3server.anderefirma.com.

Konfiguration

Allgemeine Konfigurationseinstellungen

Wie auch bei den anderen Protokollen dieses Geräts können Sie die Einstellungen für dieses Protokoll aus einer Reihe typischer Situationen auswählen oder Sie können verschiedene Einstellungen genau Ihren Vorstellungen anpassen. Zu den Einstellungen gehören:

- Port-Nummer
- Anzahl der Listener.
  Das Gerät kann über eine beliebige Anzahl von Instanzen des Proxy verfügen, die den Verkehr empfangen. Wenn Sie diese Zahl erhöhen, steigern Sie somit die Anzahl der Transfers, die das Gerät gleichzeitig durchführen kann. Es gibt jedoch eine Grenze, bei der weitere Steigerungen die Leistung nicht mehr verbessern. Der Wert wird unter Umständen von anderen Proxy-Servern beeinflußt, die unterschiedliche Protokolle scannen, d. h. er ist von der gesamten Auslastung abhängig.
- Anzahl der Verbindungen pro Listener.
  Das Gerät kann über eine beliebige Anzahl gleichzeitiger Verbindungen für jede Instanz des Proxy verfügen. Jeder Proxy kann auch mehrere Verbindungen gleichzeitig handhaben. Dieser Wert entspricht der obengenannten Anzahl der Listener.
- Speichermenge pro Verbindung (für Virenscan zugewiesen).
  Das Gerät weist einen Speicherbereich für Virenscans zu. Wenn dieser Bereich überschritten wird, werden Mitteilungen auf der Festplatte gespeichert. Der Wert wird unter Umständen von anderen Proxy-Servern beeinflußt, die unterschiedliche Protokolle scannen, d. h. er ist von der gesamten Speicherverfügbarkeit abhängig.

Jede Einstellung verfügt über einen ursprünglichen Standardwert. Wenn Sie verschiedene neue Einstellungen ausprobieren, diese aber nicht zu optimalen Ergebnissen führen, können Sie die Standardwerte einfach wiederherstellen, da das Gerät sie beibehält.

Virenscan 7

Einführung

Das Gerät verwendet das Antiviren-Scanmodul von McAfee, das über folgende Funktionen verfügt:

- Entdecken und Entfernen von Viren
- Automatisches Scannen komprimierter Dateien
- Automatisches Dekomprimieren und Scannen von Dateien, die in folgenden Dateien komprimiert wurden: PKZip, .LHA und .ARJ.
- Entdecken von Makro-Viren
- Einfache Aktualisierung mit neuen Antiviren-Technologien
- Entdecken polymorpher Viren
- Entdecken neuer Viren in ausführbaren Dateien und zusammengesetzten OLE-Dokumenten mit Hilfe einer Methode, die *heuristische Analyse* genannt wird.

Die heuristische Analyse

Ein Virenscanner verwendet zwei Methoden, um Viren aufzuspüren: Signaturen und heuristische Analysen. Eine *Virussignatur* ist einfach ein binäres Muster, das in einer von einem Virus befallenen Datei gefunden wird. Der Virenscanner verwendet die Daten in seinen Virusdefinitionsdateien, um nach diesen Mustern zu suchen. Bei dieser Methode kann kein neuartiger Virus entdeckt werden, da dessen Signatur noch nicht bekannt ist. Aus diesem Grund wird eine weitere Methode verwendet, die als *heuristische Analyse* bezeichnet wird.

Programme, die einen Virus enthalten, weisen häufig ganz bestimmte Eigenschaften auf. Sie versuchen unaufgefordert, Dateien zu modifizieren, aktivieren E-Mail-Clients oder versuchen auf eine andere Weise, sich selbst zu verbreiten. Der Virenscanner analysiert den Programmcode, um solche Computeranweisungen aufzuspüren. Er versucht, rechtmäßiges Verhalten zu erkennen. Beispielsweise wird beim Benutzer nachgefragt, bevor eine Aktion ausgeführt wird, wodurch ein falscher Alarm vermieden werden kann.

Einige Viren sind verschlüsselt, damit sie nicht entdeckt werden können. Jede Computeranweisung ist einfach eine binäre Zahl, aber der Computer verwendet nicht alle möglichen Zahlen. Der Virenscanner sucht deshalb nach unerwarteten Zahlen in einer Programmdatei, um einen verschlüsselten Virus zu entdecken.

Mit Hilfe dieser Techniken können die Virenscanner sowohl bekannte als auch viele neue Viren und deren Varianten aufspüren.

Sicherheitsstufen

Nicht alle Dateien sind anfällig für Viren. So sind Textdateien beispielsweise nur Daten; sie werden nicht als ausführbarer Computercode ausgeführt und können aus diesem Grund keine Viren verbreiten. Komprimierte Dateien können ebenfalls keine Viren verbreiten, außer sie werden zuerst dekomprimiert und dann ausgeführt. Wenn Sie zusätzlich andere Virenscantechniken verwenden (beispielsweise Scannen bei Zugriff, wobei Viren beim Öffnen und Ausführen von Dateien aufgespürt werden), sind einige der höheren Scan-Stufen (die mehr Zeit erfordern) nicht erforderlich. Aus diesem Grund bietet das Gerät unterschiedliche Sicherheitsstufen beim Virenschutz. Sie können eine hohe, mittlere und niedrigere Scan-Stufe wählen:

- Hoch – Höchste Sicherheit. Alle Dateien, einschließlich der komprimierten Dateien, werden gescannt.
- Mittel – Es werden ausführbare Dateien, Microsoft Office-Dateien und komprimierte Dateien gescannt.
- Niedrig – Geringste Sicherheit. Es werden ausführbare Dateien und Microsoft Office-Dateien gescannt.

Handhabung infizierter Nachrichten

Die Antiviren-Software des Geräts entdeckt Viren in allen möglichen Arten elektronischen Datenaustausches.

Im Fall von HTTP und FTP werden Inhalte, die nicht gesäubert werden können, abgeblockt. Sie können deshalb nicht gesäubert oder gelöscht werden, weil sich das Original auf einem anderen Server befindet.

Im Fall von SMTP scannt das Gerät die Anlagen. Wenn hier die angehängte Datei nicht gesäubert werden kann, wird sie durch eine Nachricht ersetzt, zum Absender zurückgeschickt oder in einen Quarantänebereich für eine spätere Untersuchung verschoben.

Das Gerät überprüft den Quarantänebereich sorgfältig. Es werden Warnungen ausgegeben, wenn der Bereich überfüllt ist, und ältere Nachrichten werden automatisch gelöscht.

Automatische Aktualisierung

Jeden Monat gibt es Hunderte neuer Viren. Um zu gewährleisten, daß Ihr Netzwerk immer geschützt ist, muß Ihre Antiviren-Software stets auf dem neuesten Stand sein. Das Gerät erleichtert dies, da die Software automatisch aktualisiert wird.

Antiviren-Software

Die Antiviren-Software besteht aus zwei Teilen:

- Virusdefinitionsdateien (DAT)
- Antiviren-Scanmodul

Beide Teile sind für den kompletten Schutz vor Computerviren wesentlich und müssen ständig aktualisiert werden.

- Die *DAT-Dateien* enthalten Beschreibungen neuer Viren und ermöglichen dem Modul, sie zu finden und zu säubern. Neue DAT-Dateien werden normalerweise wöchentlich, manchmal auch häufiger zur Verfügung gestellt.
- Das *Modul* enthält die Software zum Verarbeiten der DAT-Dateien. Da neue *Typen* von Viren auftreten, muß das Modul möglicherweise verbessert werden, um sie zu beseitigen. Wenn ein veraltetes Modul aktuelle DAT-Dateien verwendet, kann es keinen vollen Nutzen aus deren aktuellen Inhalten ziehen. Die Moduldatei wird nicht so häufig aktualisiert wie die DAT-Dateien – normalerweise alle paar Monate.

Sowohl die DAT-Dateien als auch das Modul können von der FTP-Site oder der Website von Network Asscociates mittels einer automatischen Aktualisierung heruntergeladen werden.

Gründe für Updates

Damit Sie über den bestmöglichen Schutz verfügen, werden die von dieser Software verwendeten Virusdefinitionsdateien (DAT) ständig aktualisiert. Die Software macht zwar von der heuristischen Analyse Gebrauch, mit der einige bisher unbekannte Viren oder schädliche Codes aufgespürt werden, doch treten häufig viele neue Virentypen und andere Virenträger auf.

Oftmals kann die vorhandene Software diese Angreifer nicht finden, da die Virusdefinitionsdateien (DAT) inzwischen veraltet sind. Um einen maximalen Schutz zu erzielen, empfehlen wir dringend, die Dateien regelmäßig (mindestens einmal pro Woche) zu aktualisieren.

Bester Zeitpunkt für Updates

Wir empfehlen dringend, die Virusdefinitionsdateien regelmäßig (mindestens einmal pro Woche) zu aktualisieren. Jede Woche werden neue DAT-Dateien herausgegeben. Manchmal werden jedoch schon vorher DAT-Dateien (sogenannte EXTRA-DATs) zur Verfügung gestellt, um auf das plötzliche Auftreten neuer Viren zu reagieren.

Sie sollten eine Uhrzeit wählen, zu der das Netzwerk nicht ausgelastet ist. Am besten eignet sich ein Zeitpunkt in der Nacht oder tagsüber außerhalb der üblichen Geschäftszeiten.

Falls in Ihrem Unternehmen auch an Wochenenden gearbeitet wird, könnten Sie die Aktualisierungen jeweils am Freitag und Sonntag abend vornehmen.

Planen von Updates

Das Gerät ermöglicht es Ihnen, mindestens einmal pro Tag von einer dieser Quellen regelmäßige Updates einzuplanen:

- Von unserem FTP-Server oder von einem anderen autorisierten Provider.
- Von einem Computer, der als Proxy fungiert, wenn Ihr Gerät auf diese Server nicht direkt zugreifen kann.
- Von einem Computer in Ihrem Netzwerk, auf den die erforderlichen Dateien bereits heruntergeladen wurden.

Die Dateien sind komprimiert, um einen schnellen Download zu gewährleisten.

Inhaltsüberwachung 8

Einführung

Das Gerät kann ein- und ausgehende E-Mails nach unerwünschten Inhalten durchsuchen. Sie können Regeln erstellen, in denen Sie festlegen, was in den Nachrichten nicht zulässig ist. Mit Hilfe dieser Regeln verhindert das Gerät, daß solche Nachrichten die beabsichtigten Empfänger erreichen.

Sie können beliebig viele Regeln festlegen, und in jeder Regel können Wörter in unterschiedlichen Kombinationen angegeben werden. Beispiel: In einer komplexen Regel ist die Verwendung eines Wortes in einer bestimmten Situation zulässig, aber in anderen Situationen nicht.

Normalerweise wird nur der Inhalt der Nachrichten durchsucht. Sie können jedoch auch den Inhalt von Anhängen überprüfen lassen. Der Ausdruck „Wörter“ betrifft auch die Namen angehängter Dateien und Dateitypen, die durch ihre Erweiterung (z. B. BMP oder JPEG) gekennzeichnet werden.

In den Beispielen des nächsten Abschnitts werden einige der vielen Möglichkeiten gezeigt, wie die Inhaltsüberwachung eingesetzt werden kann. Ausführlichere Informationen zu Regeln finden Sie in den nachfolgenden Abschnitten.

Beispiele für Regeln

Mit Hilfe der Inhaltsüberwachung können Sie Regeln erstellen, die das Auftreten von Wörtern und Ausdrücken in vielen Situationen und Kombinationen (siehe nachfolgende Beispiele) erkennen.

- Vertraulicher Umgang mit Informationen
- Verringern der Netzwerkbelastung
- Abblocken beleidigender Wörter
- Abblocken belästigender E-Mails
- Verringern von Ablenkungen

In jedem hier beschriebenen Beispiel können E-Mails abgeblockt werden – indem sie zerstört oder in einen Quarantänebereich verschoben werden, in dem sie später noch untersucht werden können. Sie müssen jedoch bei der Handhabung von E-Mails die geltende Rechtsprechung berücksichtigen.

Vertraulicher Umgang mit Informationen

Wenn es in Ihrem Unternehmen üblich ist, daß ein neues Ereignis, Produkt oder Projekt nicht außerhalb der Firma besprochen werden soll, können Sie verhindern, daß der entsprechende Name in ausgehenden E-Mails erwähnt wird.

Beispiel: Ihre Firma möchte ein neues Produkt mit dem Namen SuperDing auf den Markt bringen. Um zu verhindern, daß außerhalb des Unternehmens jemand von dem Produkt erfährt, muß dieses Wort in jeder E-Mail erkannt werden.

Aus diesem Grund erstellen Sie eine Regel mit der Bezeichnung „Vertrauliche Informationen über SuperDing“ und wenden diese Regel auf Textanhänge, den Textteil und die Betreffzeile von Nachrichten an. Sie geben das Wort „SuperDing“ als das Wort an, das als Auslöser dieser Regel fungiert.

Zweites Beispiel: Ihr Unternehmen möchte das neue Produkt im Januar auf den Markt bringen. Dieses Datum muß geheimgehalten werden. Nachrichten der folgenden Art dürfen nicht aus dem Unternehmen an die Öffentlichkeit gelangen:

```
Wir können „SuperDing“ im Januar auf den Markt bringen.
```

Vor diesem Datum werden in weniger brisanten E-Mails die Details und Vorbereitungen für den Marktstart des Produkts besprochen. Andere Produkte werden ebenfalls auf den Markt gebracht, doch deren Daten sind von geringerer Wichtigkeit. Nachrichten dieser Art sollten nicht abgeblockt werden:

```
Tagesordnung für die morgige Sitzung:
1. Fortschritte beim Marktstart von „SuperDing“
2. So können wir unsere Kosten für Bürobedarf senken
3. Marktstart von „MegaBox“ im Januar
```

Sie können eine Regel erstellen, die nur dann ausgelöst wird, wenn beide Wörter – „SuperDing“ und „Januar“ – nahe beieinander stehen (z. B. innerhalb 30 Zeichen).

Letztes Beispiel: Ihr Unternehmen möchte Herrn Mustermann zum Aufsichtsratsvorsitzenden befördern. Die von Ihnen erstellte Regel muß bei der Kombination der beiden Wörter „Aufsichtsratsvorsitzender“ und „Mustermann“ ausgelöst werden.

Verringern der Netzwerkbelastung

Die Übertragung einiger Dateitypen, beispielsweise von Filmdateien (MPEGs) und Bitmap-Grafiken, können eine große Belastung für Netzwerke darstellen. Sie können eine Liste mit nicht zulässigen Dateierweiterungen erstellen, um deren Verwendung einzuschränken. Die auslösenden Wörter können „.BMP“ oder „.MPG“ lauten und so eingestellt werden, daß sie nur die Namen von Anhängen betreffen.

Abblocken beleidigender Wörter

Nachrichten beleidigender Art von Ihren Mitarbeitern oder Kunden können dem Ruf Ihrer Firma schaden. Sie können eine Liste mit nicht zulässigen Wörtern erstellen, um deren Verwendung zu verhindern.

Stellen Sie sich beispielsweise den Ausdruck „Sie sind ein falscher Hund“ vor. In einem anderen Kontext, z. B. bei der Erläuterung einer Hunderasse (z. B. Dackel oder Schäferhund), ist dieses Wort nicht beleidigend. Um zu verhindern, daß dieses Wort in seinem beleidigenden Kontext an Ihre Firma geschickt wird oder sie verläßt, erstellen Sie eine neue Regel mit der Bezeichnung „Beleidigung – Hund“. Sie legen die Regel so fest, daß sie auf den Textteil der Nachricht angewendet wird. Zudem bestimmen Sie, daß solche Nachrichten gelöscht werden. Nach der Eingabe des Wortes „Hund“ können Sie den Kontext weiter verfeinern. Sie können beispielsweise festlegen, daß diese Regel nur ausgelöst wird, wenn keines der Wörter Schäferhund, Dackel, Spaniel usw. ebenfalls in der Nachricht vorkommt.

Abblocken belästigender E-Mails

Verärgerte ehemalige Angestellte, Versender von Hoaxes und rücksichtslose Verkäufer, die die E-Mail-Adressen Ihrer Mitarbeiter kennen, können Probleme verursachen.

Beispiel: Johannes Schmidt hat Mitarbeiter Ihrer Firma belästigt, indem er ihnen unerwünschte E-Mails gesendet hat. Der Inhalt seiner Nachrichten ist zwar unterschiedlich, doch er verwendet immer eine von zwei E-Mail-Adressen. Sie erstellen eine Regel mit der Bezeichnung „Lästige Person“. Geben Sie als auslösenden Ausdruck die beiden E-Mail-Adressen von Johannes Schmidt ein, und wenden Sie die Regel nur auf den Absender der Nachricht an.

Das Gerät enthält eine Anti-Spam-Funktion, die verhindert, daß bekannte Spam-Quellen Ihr Netzwerk angreifen können. Sie können jedoch auch den Inhalt nach verbreiteten oder bekannten Ausdrücken durchsuchen lassen, um diese Art von Angriffen weiter einzuschränken. Ausdrücke, wie beispielsweise „so werden Sie schnell reich“ oder „dieser Virus wird Ihren Computer zerstören“, können als auslösende Ausdrücke für eine andere Regel fungieren.

Verringern von Ablenkungen

Wenn häufige unangebrachte Nachrichten Ihre Mitarbeiter ablenken, kann das Gerät diese Nachrichten abblocken und deren Absender davon abhalten, dies wieder zu tun.

Beispiel: Werbung per E-Mail mit der Betreffzeile „Auto zu verkaufen“ oder „Haus zu verkaufen“. Nachrichten dieser Art nehmen Ihre E-Mail-Ressourcen unnötig in Anspruch und lenken Ihre Mitarbeiter ab. Um solch eine E-Mail abzublocken, erstellen Sie eine Regel mit der Bezeichnung „Ablenkende Werbung“. Legen Sie als auslösenden Ausdruck „zu verkaufen“ fest, und wenden Sie die Regel nur auf die Betreffzeile von Nachrichten an.

Viele Spiele werden per E-Mail als Computerprogramme (EXE-Dateien) gesendet. Sie können solche Dateien abblocken, indem Sie eine Regel erstellen, die ausgelöst wird, wenn Anhänge mit der Dateierweiterung „.exe“ gesendet werden. Diese Regel hat zudem einen weiteren Vorteil: Spiele werden häufig verwendet, um Viren zu verbergen.

Erstellen von Regeln

Damit Sie die Inhaltsüberwachung anwenden können, müssen Sie *Regeln* erstellen. Gehen Sie dabei folgendermaßen vor:

- Festlegen einer Bezeichnung für eine Regel.
- Festlegen eines Anwendungsbereichs der Regel.
- Festlegen der auszuführenden Aktion bei Auslösung der Regel.
- Festlegen des Wortes oder Ausdrucks, das/der erkannt werden soll.
- Optionale fortgeschrittene Funktionen.

Diese Schritte werden im folgenden ausführlicher beschrieben.

Festlegen einer Bezeichnung für eine Regel

Im Laufe der Zeit werden Sie möglicherweise viele Regeln erstellen. Aus diesem Grund ist es empfehlenswert, für jede Regel eine sinnvolle Beschreibung anzugeben.

Festlegen eines Anwendungsbereichs der Regel

Ein zu sperrender Ausdruck befindet sich unter Umständen im Haupttextteil der Nachricht, in der Betreffzeile oder sogar innerhalb eines einfachen Textanhangs. Das Gerät kann auch den Dateinamen von Anlagen durchsuchen, damit Sie Anlagen nach dem genauen Namen (z. B. „gutesspiel.exe“) oder nach Dateityp (z. B. *.MPG-Dateien) abblocken können. Das Durchsuchen bei jedem Nachrichtenabsender blockt bekannte Absender (insbesondere solche, die *belästigende* E-Mails schicken) ab. Weitere Informationen hierzu finden Sie im Abschnitt über die Anti-Spam-Funktionen.

Festlegen der auszuführenden Aktion bei Auslösung der Regel

Sie können eine von zwei Aktionen für Nachrichten wählen, die eine Regel auslösen.

- Nachricht wird gelöscht – Der Empfänger erhält die Nachricht nicht.
- Nachricht wird in Quarantänebereich verschoben – Der Empfänger erhält die Nachricht nicht. Die E-Mail wird in einen Quarantänebereich verschoben. Dort können Sie die E-Mail prüfen und danach weiterleiten oder löschen.

Festlegen des Wortes oder Ausdrucks, das/der erkannt werden soll

Sie können ganz genau festlegen, wie ein Wort oder Ausdruck angezeigt wird, indem Sie Groß-/Kleinschreibung angeben, Platzhalter verwenden und die Position bestimmen:

- **Groß-/Kleinschreibung ignorieren**
  Normalerweise wird nach dem Wort bzw. dem Ausdruck genauso gesucht, wie es/er angegeben wurde. Wenn Sie festlegen, daß Groß-/Kleinschreibung ignoriert werden soll, wird das Wort bzw. der Ausdruck unabhängig von Groß-/Kleinschreibung als übereinstimmend angesehen. So wird abc mit abc, Abc, ABC und aBc oder jeder anderen Kombination mit Groß-/Kleinschreibung in diesem Ausdruck als übereinstimmend angesehen.

- **Platzhalter** verwenden
  Bei dieser Funktion können Sie die Zeichen * und ? verwenden, um fehlende Zeichen darzustellen.

  ? steht für ein einzelnes Zeichen.
  Beispiel: „??nd“ kann für „Sand“, „Hund“ oder „Mond“ stehen.

  * steht für eine beliebige Anzahl an Zeichen (auch für gar kein Zeichen).
  Beispiel: „l*eben*“ kann für „leben“, „lebendig“ und „lieben“ stehen.

- **Zeichen am Wortanfang oder -ende angeben**
  Sie können Zeichen finden, die nur am Anfang eines Wortes stehen.
  Beispiel: „Mut“ findet „Mut“, „Mutter“ und „Mutant“.

  Sie können Zeichen finden, die nur am Ende eines Wortes stehen.
  Beispiel: „rad“ findet „Fahrrad“ und „Grad“.

Optionale fortgeschrittene Funktionen

Sie können die Bedingungen zum Auslösen einer Regel weiter verfeinern, indem Sie festlegen, wie viele Wörter oder Ausdrücke in Kombination mit dem ersten Wort bzw. Ausdruck auftreten dürfen (*Kontext* und *Nähe* zueinander).

Kontext

- Eine Regel kann ausgelöst werden, wenn ALLE zusätzlichen Wörter oder Ausdrücke vorkommen.

  Beispiel: Eine Regel wird ausgelöst, wenn der Name eines geheimen neuen Produkts und das Datum seiner Markteinführung in der gleichen E-Mail auftreten.

- Eine Regel kann ausgelöst werden, wenn IRGENDWELCHE zusätzlichen Wörter oder Ausdrücke vorkommen.

  Beispiel: Eine Regel wird ausgelöst, wenn ein beliebiges Wort auftritt, das in einer Liste mit beleidigenden Wörtern oder einer Liste mit geheimen Projekten steht.

- Eine Regel kann ausgelöst werden, wenn KEINES der zusätzlichen Wörter oder Ausdrücke vorkommt.

  Beispiel: Eine Regel wird ausgelöst, wenn eine Beleidigung (z. B. der Name eines Tieres – beispielsweise eines Hundes) verwendet wird, außer wenn es dazu verwendet wurde, um eine bestimmte Rasse dieses Tieres (z. B. einen Dackel oder einen Schäferhund) zu beschreiben.

Nähe

Wenn Sie normalerweise nach gesperrten Inhalten suchen, befinden sich die gesperrten Wörter nahe beieinander. In einem sehr langen Dokument können die Wörter trotzdem unabhängig voneinander auftreten und fälschlicherweise die Regel auslösen. Um diesen Fall zu vermeiden, muß diese Regel die Nähe der Wörter berücksichtigen. Eine Regel kann beispielsweise nur dann ausgelöst werden, wenn zwei Wörter mit einem Abstand von höchstens 50 Zeichen auftreten.

Warnungen 9

Einführung

Das Gerät generiert eine große Anzahl von Warnungen, die von Ereignissen folgender Art verursacht werden:

- Entdeckung eines Virus
- Entdeckung eines gesperrten Wortes oder Ausdrucks
- Entdeckung einer Spam-E-Mail
- Fehlgeschlagene Anmeldung
- Ressourcen-Engpässe

Sie können festlegen, wie diese Warnungen ausgegeben werden – in Form von E-Mails, SNMP-Warnungen oder ePolicy Orchestrator-Ereignissen. Zudem können Sie die Detailstufe für die jeweilige Methode bestimmen.

Ein Protokoll im Gerät zeichnet die Ereignisse außerdem über viele Wochen oder sogar Monate hinweg auf. Die gesammelten Daten können als Diagramme und Berichte dargestellt werden. Weitere Informationen hierzu finden Sie unter „Berichte und Diagramme“ auf Seite 69.

Informationsverteilung

Das Gerät erzeugt eine große Menge an Informationen, die Sie auf verschiedenen Wegen verteilen können – in Form von E-Mails, SNMP-Warnungen oder ePolicy Orchestrator-Ereignissen.

- **E-Mails**
  Diese Informationen werden per E-Mail an eine beliebige Anzahl von Empfängern gesendet.
- **SNMP-Traps**
  Diese Informationen werden als Warnungen an einen SNMP-Manager (Simple Network Management Protocol) gesendet. Die MIB-Datei des Geräts teilt dem SNMP-Manager mit, wie die Daten in den Traps interpretiert werden.
- **ePolicy Orchestrator-Ereignisse von McAfee**
  Ein im Gerät installiertes Agentenprogramm leitet die Informationen an einen ePolicy Orchestrator-Server weiter, der die Aktivitäten des Geräts und die Antiviren-Aktivitäten von Computern in einem gesamten Netzwerk überwachen und auswerten kann.

Festlegen von Details

Sie können die Auswahl der Ereignisse für jede Methode folgendermaßen verfeinern:

- Geben Sie die Priorität des Ereignisses an, das weitergeleitet werden soll – beispielsweise, daß es sich um eine Erkennung oder wichtige Warnung handelt.
- Geben Sie die Rolle des Empfängers an – beispielsweise, daß es sich um einen Maintainer oder Administrator handelt.
- Bestimmen Sie einen Code für das Ereignis (die Ereignis-ID) – auf diese Weise können Sie genau festlegen, was überwacht werden soll.

Überwachen kritischer Stufen

Das Gerät überwacht einige seiner E-Mail-Ressourcen, um sicherzustellen, daß diese nicht überlastet werden. Beispiel:

- Größe eingehender und ausgehender Virus-Quarantänebereiche.
- Größe eingehender und ausgehender Inhalts-Quarantänebereiche
- Größe der Warteschlange zurückgestellter E-Mails

Sie können das Gerät so konfigurieren, daß ein Administrator eine Warnung erhält, wenn die Ressourcen knapp werden. Aktivieren Sie hierzu die E-Mail-Warnung, und konfigurieren Sie sie so, daß Informationen über alle Warnungen und kritischen Ereignisse weitergeleitet werden.

Umgang mit E-Mail-Problemen

Das Gerät kann einen Administrator (oder „Postmaster“) zuweisen, um Anfragen von Absendern bezüglich E-Mails zu beantworten, die aufgrund eines Virus oder ihres Inhalts zurückgeschickt wurden.

Der Postmaster muß jemand sein, der E-Mails regelmäßig liest. Neben den Namen einzelner Benutzer können Sie auch Namen von Verteilerlisten verwenden, da das Gerät nicht zwischen ihnen unterscheiden kann. Wenn Sie ein E-Mail-Hilfsprogramm wie beispielsweise Microsoft Outlook oder Lotus Notes verwenden, können Sie Regeln einrichten, um E-Mails weiterzuleiten, wenn Sie nicht im Büro sind.

Berichte und Diagramme 10

Einführung

Das Gerät erzeugt eine große Menge an Informationen, die Sie in einem Protokoll speichern oder auf verschiedene Arten verteilen können: in Form von E-Mails, SNMP-Warnungen oder ePolicy Orchestrator-Ereignissen (siehe „Warnungen“ auf Seite 67).

Informationen im Protokoll

Das Protokoll im Gerät zeichnet Aktivitäten über viele Wochen oder sogar Monate hinweg auf und ermöglicht es Ihnen, folgende Informationsarten darzustellen:

- Entdeckte Viren und gegen sie ausgeführte Aktionen – unabhängig davon, ob die infizierten Dateien gesäubert, gelöscht oder in einen Quarantänebereich verschoben wurden.
- Gesperrte Websites. Zugriffsversuche auf gesperrte Websites, die für Geschäftszwecke als unpassend angesehen werden.
- Spam. Vorkommnisse von Spam-Mail mit Datum, Uhrzeit und Absender.
- E-Mail-Inhaltsregeln. Regeln, die ausgelöst wurden, weil gesperrte Inhalte in einer E-Mail vorkamen.
- Verwaltungsereignisse wie beispielsweise fehlgeschlagene Anmeldungsversuche und Dienstausfälle.

Die Informationen können vom Gerät im CSV-Format (als kommagetrennte Datei) exportiert werden. Dieses Format wird von Tabellenkalkulationsprogrammen wie beispielsweise Microsoft Excel und Lotus 123 unterstützt.

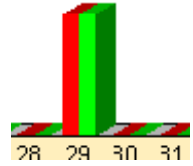
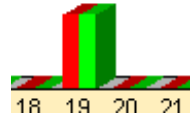
Sie können die Detailtiefe und die beabsichtigte Zielgruppe festlegen und bestimmen, ob bestimmte Ereignisse überwacht werden. Die generierten Informationen können auch gefiltert werden. Sie können beispielsweise die Informationen so einschränken, daß nur Vorkommnisse eines ganz bestimmten Virus angezeigt werden.

Drilldown bei den Informationen durchführen

Die Informationen, die vom Gerät protokolliert werden, können auf verschiedene Arten grafisch dargestellt werden: als Balkendiagramme, Kreisdiagramme und Tabellen. Zudem sind die Informationen sehr detailliert, d. h. Sie können sie auf verschiedenen Ebenen untersuchen. Dieser Untersuchungsvorgang, bei dem Informationen immer detaillierter untersucht werden, wird als *Drilldown* bezeichnet. Bei einer hohen Ebene können Sie beispielsweise sehen, an welchen Tagen in einem bestimmten Monat die meisten Viren auftraten. Auf der niedrigsten Ebene können Sie das genaue Datum und die Uhrzeit jedes Vorkommnisses, den Namen des Virus und die Aktion, die vom Gerät dagegen ausgeführt wurde, anzeigen.

In den folgenden Beispielen ist ein *Drilldown* in einem Balken- und einem Kreisdiagramm zu sehen.

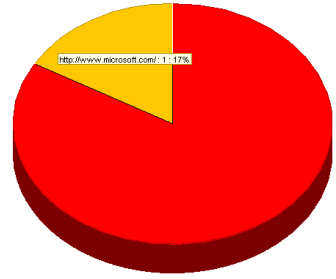
Tabelle 10-1. Beispiel für Drilldown

Beim Balkendiagramm, das die Aktivitäten eines Monats zeigt, können Sie auf einen Balken klicken, der einen Tag darstellt.	
Beim nächsten Balkendiagramm, das die Ereignisse in jeder Stunde zeigt, können Sie auf einen Balken klicken, der eine bestimmte Stunde darstellt.	
Abschließend können die Ereignisse im einzelnen angezeigt werden. Jedes verfügt über eine Datums- und eine Zeitangabe.	

Uhrzeit	Ausgeführte Aktion	Name der Website	Quelladresse
18:43:25 17/Sep/2001	Zugriff verweigert	http://www.ebay.com/	172.16.3.4
16:58:10 14/Sep/2001	Zugriff verweigert	http://www.ebay.com/	172.16.4.132

Tabelle 10-1. Beispiel für Drilldown (*Fortsetzung*)

Beim Kreisdiagramm können Sie auf ein Segment klicken.



Abschließend können die Ereignisse im einzelnen angezeigt werden. Jedes verfügt über eine Datums- und eine Zeitangabe.

Uhrzeit	Ausgeführte Aktion	Name der Website	Quelladresse
18:43:25 17/Sep/2001	Zugriff verweigert	http://www.ebay.com/	172.16.3.4
16:58:10 14/Sep/2001	Zugriff verweigert	http://www.ebay.com/	172.16.4.132

CSV-Format

Die Protokollierungsinformationen des Geräts können im CSV-Format (als kommagetrennte Datei) exportiert werden.

Eine sehr vereinfachte Form des CSV-Formats wird nachfolgend gezeigt:

```
Uhrzeit, Ereignisdatum, Ereignis-ID, Ereignistext, Grund
12:55:07,12/12/2001,18100,„Virus gefunden“,Ripper
12:55:30,12/12/2001,18100,„Virus gefunden“,Love Letter
```

Das CSV-Format ist ideal zum Importieren in ein Tabellenkalkulations- oder Datenbankprogramm wie beispielsweise Microsoft Excel, Microsoft Access oder Lotus 123. Mit diesen Programmen können Sie die Daten weiterbearbeiten und Berichte erstellen.

Wartung des Geräts 11

Einführung

Für die Wartung des Geräts ist nach der Installation und Wartung kein großer Aufwand erforderlich. Der Zugriff auf dieses Gerät ist ausschließich über einen sicheren HTTPS-Link möglich. Das hervorragend geschützte Betriebssystem verhindert außerdem nicht autorisierten Zugriff auf das interne Dateisystem. Damit die Effektivität des Geräts erhalten bleibt, muß die Software jedoch von Zeit zu Zeit geändert werden. Die Funktionen, die Ihnen beim Warten des Systems behilflich sind, werden nachfolgend beschrieben.

- **Installieren von Service Packs und Hot-Fixes**
  Mit dieser Funktion können Sie schnell und problemlos die Software des Geräts aktualisieren. Der Zugriff auf die neue Software ist von einer Website oder von Dateien auf einem anderen Computer aus möglich.

- **Installieren von ePolicy Orchestrator-Agent**
  ePolicy Orchestrator ermöglicht es Ihnen, Virusaktivitäten zu überwachen und Antiviren-Software von einem einzigen Punkt aus zu verteilen. Ein Agent-Programm, das Sie installieren können, ermöglicht es dem Gerät, seinen Status an einen zentralen Server zu übermitteln. Der Zugriff auf das Agent-Programm ist von einer Website oder von Dateien auf einem anderen Computer aus möglich.

- **Speichern und Wiederherstellen von Systemeinstellungen**
  Sie können Details zur Konfiguration des Geräts offline sicher speichern und die Informationen gegebenenfalls wiederherstellen. Der Zugriff auf die neue Software ist von einer Website oder von Dateien auf einem anderen Computer aus möglich. Die Konfigurationseinstellungen des Systems werden in einer ZIP-Datei gespeichert, die hauptsächlich XML-Dateien und zugehörige DTD-Dateien enthält. Die ZIP-Datei ist normalerweise nicht größer als 100 Kilobyte.

- **Speichern von Systemprotokollen**
  Das Gerät speichert Informationen zu zahlreichen Ereignissen wie beispielsweise Viruswarnungen und fehlgeschlagenen Anmeldungsversuchen, die Sie vom Gerät laden sowie als Berichte und Diagramme anzeigen können. Sie können diese Informationen jederzeit abfragen, um sie zu untersuchen oder zu archivieren. Die Protokollinformationen werden in einer ZIP-Datei gespeichert, die hauptsächlich Textdateien enthält. Die ZIP-Datei kann mehrere Megabyte groß sein. Sie können die Größe der Systemprotokolle einschränken. Wenn Sie beispielsweise zehn Tage festlegen, enthält das Protokoll ausschließlich Informationen über die letzten zehn Tage.

- **Automatisches Löschen überflüssiger Dateien und Informationen**
  Dateien, die sich aufgrund von Viren oder gesperrten Inhalten im Gerät befinden, füllen kontinuierlich den Quarantänebereich des Geräts auf. Das Gerät entfernt automatisch alte Dateien und Informationen des Systemprotokolls, die für einen bestimmten Zeitraum gespeichert waren. Informationen werden üblicherweise 14 Tage lang im Gerät gespeichert.

- **Ausschalten oder Neustarten des Geräts**
  Das Gerät kann per Fernzugriff neu gestartet oder sogar komplett ausgeschaltet werden. Um unerlaubte oder versehentliche Änderungen zu vermeiden, ist das Ausführen dieser Funktion nur unter Angabe eines Kennworts möglich.

- **Status**
  Informationen zum Gerätestatus (beispielsweise die Version der Antiviren-Software) sind sofort verfügbar. Andere nützliche Informationen (beispielsweise der Zeitpunkt des letzten Neustarts und die Laufzeit) sind ebenfalls erhältlich.

Konfiguration

Wenn das Gerät am Anfang so eingerichtet wird, wie im Installationshandbuch beschrieben, müssen verschiedene Parameter festgelegt werden. In den folgenden Abschnitten finden Sie Informationen zu diesen Parametern.

Hostname des Geräts

Das Gerät weist einen standardmäßigen Hostnamen auf, entweder „webshielde250“ (WebShield e250) oder „webshielde500“ (WebShield e500). Unter diesem Namen wird es im Netzwerk gekennzeichnet. Falls Sie McAfee ePolicy Orchestrator verwenden, ist dies auch der Name, der von ePolicy Orchestrator zur Kennzeichnung des Geräts verwendet wird.

Sie können diesen Namen auch in einen eindeutigen Namen mit nicht mehr als 15 Zeichen ändern. Falls Sie ein weiteres Gerät im gleichen Netzwerk einsetzen, müssen Sie den Namen ändern, damit die Geräte über eindeutige Namen verfügen.

TIP: Es wird empfohlen, den Hostnamen in einen eindeutigen Namen zu ändern, der bei einer umgekehrten Suche in Ihrem DNS-Server angegeben wird. Falls Sie ePolicy Orchestrator verwenden (dieses Programm ist separat erhältlich), ist dies auch der Name, der von ePolicy Orchestrator zur Kennzeichnung des Geräts verwendet wird.

Darüber hinaus können Sie durch Ändern des Namens verhindern, daß das Gerät zu einem potentiellen Ziel für Hacker wird.

Domäne

Geben Sie die Domäne oder Subdomäne ein, in der sich das Gerät befindet. Die Domäne oder Subdomäne muß vollständig qualifiziert und auf dem vom Gerät verwendeten lokalen DNS-Server eingegeben sein (oder einem Server, auf den der lokale DNS-Server verweist), da das Gerät diesen DNS-Server verwendet, um sich selbst zu identifizieren.

Netzwerkadressen

Sie müssen Informationen zu der TCP/IP-Netzwerkadresse für das Gerät angeben (beispielsweise eine IP-Adresse und eine Subnet-Maske), so daß dieses mit dem Netzwerk kommunizieren kann, mit dem es verbunden ist.

Das Gerät verwendet den lokalen DNS-Server für folgende Aktivitäten:

- Versuch, gescannte SMTP-E-Mail-Nachrichten zuzustellen, falls die DNS-Methode ausgewählt ist.
- Überprüfen von Anfragen beim Surfen im Internet (HTTP) und Ermitteln, welche URLs blockiert werden sollen, falls das Blockieren von URLs konfiguriert ist.

Sie müssen dem Gerät eine neue IP-Adresse für den Daten-Port bereitstellen, die für Ihr Netzwerk geeignet ist. Die IP-Adresse des Verwaltungs-Ports müssen Sie jedoch nicht ändern (die Standardadresse lautet 10.1.2.108).

Im Installationshandbuch wird gezeigt, wo sich die Daten- und Verwaltungs-Ports an Ihrem Gerät befinden.

Interne Netzwerke

Stellen Sie die Domänen oder IP-Adressen für die internen Netzwerke bereit (innerhalb Ihres Unternehmens), mit denen das Gerät kommuniziert. Sie können beliebig viele Netzwerke angeben. Sie können Domänennamen verwenden, da das Gerät umgekehrte DNS-Server-Suchen durchführen kann, um die Hosts zu überprüfen.

❑ **HINWEIS:** Schließen Sie die Domäne ein, in der sich das Gerät befindet, es sei denn, diese Domäne soll als externes Netzwerk behandelt werden.

Externe Netzwerke

Das Gerät verwendet eine *-Domäne, um alles, was nicht als internes Netzwerk festgelegt wurde, als externes Netzwerk zu kennzeichnen. Falls Sie bestimmte interne Subdomänen haben, die als externe Netzwerke behandelt werden sollen, beispielsweise `test.meinefirma.com`, kennzeichnen Sie diese Subdomänen als externe Netzwerke.

Geben Sie die Domänen oder IP-Adressen für die externen Netzwerke an (außerhalb Ihres Unternehmens), mit denen das Gerät kommuniziert. Sie können beliebig viele Netzwerke angeben. Sie können Domänennamen verwenden, da das Gerät umgekehrte DNS-Server-Suchen durchführen kann, um die Hosts zu überprüfen.

WARNUNG: Es wird empfohlen, den *-Domäneneintrag in Ihren externen Netzwerken zu behalten, weil dadurch sichergestellt wird, daß das Gerät stellvertretend Datenverkehr für das Internet empfängt.

Protokolle

Das Gerät läßt standardmäßig Proxies für die unterstützten Protokolle zu (so daß deren Datenverkehr passieren kann) und prüft den gesamten Datenverkehr in beiden Richtungen (eingehend und ausgehend) auf Viren. Sie können die Proxies für die Protokolle deaktivieren, die Sie blockieren möchten. Dies ist möglich, wenn Sie diese Protokolle mit einem anderen Gerät scannen.

Beim Konfigurieren der einzelnen Protokolle in der Benutzeroberfläche des Geräts können Sie die Ports angeben, die von Ihrem Netzwerk zur Übertragung der Protokolldaten verwendet werden (falls sie vom Standard abweichen), und die Virenprüfung für dieses Protokoll in eine Richtung (eingehend oder ausgehend) deaktivieren.

HINWEIS: Das Gerät scannt Mail-Downloads (POP3), ohne die Richtung (eingehend oder ausgehend) zu ermitteln (siehe „Mail-Download (POP3)“ auf Seite 79). Aus diesem Grund gibt es nur ein Kontrollkästchen.

„Scanning profile“ (Scan-Profil)

Das Gerät teilt seine Ressourcen gemäß der erwarteten Verwendungshäufigkeit zwischen den Protokollen auf. In der Benutzeroberfläche des Geräts können Sie eines der folgenden Verwendungsprofile auswählen, um die Häufigkeit einzustellen.

- High constant SMTP, some HTTP, minimal FTP (SMTP konstant hoch, manchmal HTTP, selten FTP).
- Moderate constant SMTP, constant HTTP, minimal FTP (SMTP konstant moderat, konstant HTTP, selten FTP).
- Very variable SMTP, constant HTTP, minimal FTP (SMTP stark schwankend, konstant HTTP, selten FTP).
- Bei vom Benutzer ausgewählten Werten verwendet das Gerät die entsprechenden Einstellungen auf den Konfigurationsseiten des Protokolls (in der Benutzeroberfläche), so daß Sie die gewünschten Konfigurationseinstellungen angeben können.

> ☐ **HINWEIS:** In den Verwendungsprofilen wird das Mail-Download-Protokoll (POP3) nicht erwähnt, da es in der Regel weniger häufig verwendet wird als die anderen Protokolle. Auf den Protokollkonfigurationsseiten (in der Benutzeroberfläche) sind jedoch – wie bei den anderen Proxies – die genauen Konfigurationseinstellungen für jedes Protokoll zur Änderung verfügbar, so daß bei Bedarf weitere Anpassungen vorgenommen werden können.

In den folgenden Abschnitten werden die zusätzlichen Informationen beschrieben, die zum Einrichten der verschiedenen Protokolle erforderlich sind: „E-Mail (SMTP)“ auf Seite 77, „Dateiübertragung (FTP)“ auf Seite 79 und „Mail-Download (POP3)“ auf Seite 79.

E-Mail (SMTP)

Bei der Zustellung von gescannten SMTP-E-Mail-Nachrichten versucht das Gerät in der angegebenen Reihenfolge eine oder mehrere der folgenden Methoden:

- **Lokal konfigurierte Domänen**
- **DNS** – Das Gerät verwendet den lokalen DNS-Server, den Sie angeben, wenn Sie die Informationen zu der TCP/IP-Netzwerkadesse angeben (siehe „Netzwerkadressen“ auf Seite 75).
- **Ersatz-Relays**

Lokal konfigurierte Domänen

Sie können Mail-Relays angeben, um für bestimmte Domänen vorgesehene E-Mail-Nachrichten an deren Mail-Server zu senden (Abbildung 11-27). Sie können beliebig viele Relays erstellen.

> **HINWEIS:** Geben Sie die gebräuchlichsten Relays zuerst an, da das Gerät die Relays der Reihe nach ausprobiert.

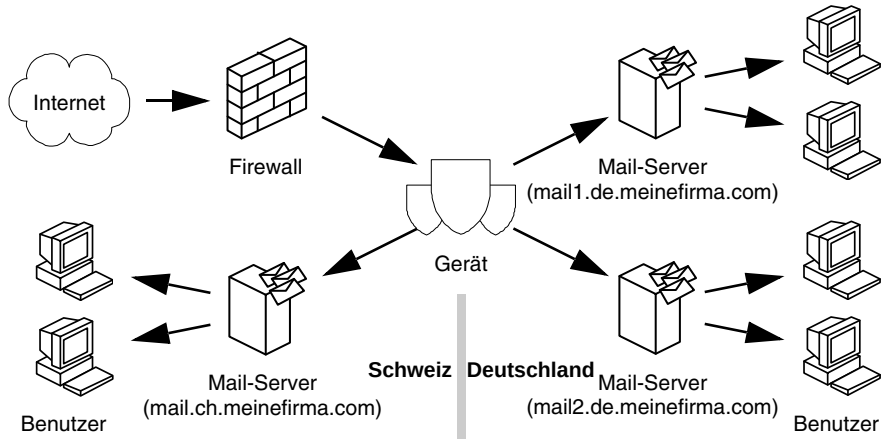


Abbildung 11-27. Mail-Relays an mehrere Mail-Server oder Gateways

Ersatz-Relays

Sie können Ersatz-Relays angeben, um E-Mail-Nachrichten weiterzuleiten, die mit Hilfe anderer Zustellungsmethoden nicht zugestellt werden konnten. Sie können beliebig viele Relays erstellen.

> **HINWEIS:** Geben Sie die gebräuchlichsten Relays zuerst an, da das Gerät die Relays der Reihe nach ausprobiert.

Weitere Informationen zu SMTP finden Sie in Kapitel 3, Seite 41.

Dateiübertragung (FTP)

Das File Transfer Protocol (FTP) ermöglicht die Übergabe von Daten zwischen Computern in zwei Modi: Binär und 8-Bit-ASCII (American Standard Code for Information Interchange). Eine binäre Übertragung ist auch zwischen Computerplattformen konsistent. Daher können die Daten effizient gescannt werden. 8-Bit-ASCII kann jedoch je nach den verwendeten Computersystemen unterschiedliche Zeichencodes und Formatierungen enthalten, so daß in diesen Daten leicht Viren verborgen werden können. Aus diesem Grund blockiert das Gerät diesen Übertragungsmodus standardmäßig, um die Sicherheit für Ihr Unternehmen zu gewährleisten. Sie können das Gerät jedoch so konfigurieren, daß es 8-Bit-Datenübertragungen zuläßt.

❑ **HINWEIS:** Manche Dienstprogramme zur Dateiübertragung verwenden standardmäßig den 8-Bit ASCII-Modus. Denken Sie daher daran, diese Dienstprogramme auf den Binärmodus umzuschalten, falls das Gerät den 8-Bit-ASCII-Modus blockiert.

Weitere Informationen zu FTP finden Sie in Kapitel 4, Seite 49.

Mail-Download (POP3)

Die E-Mail-Abrufmethode „Post Office Protocol Version 3 (POP3)“ ermöglicht das Herunterladen (Herunterziehen) von E-Mail-Nachrichten von einem Postfach auf einem Remote-Server. Es gibt zwei Betriebsmodi:

- **Generischer Proxy** – Ermöglicht die Verbindung zu einem beliebigen POP3-Server, unterstützt jedoch das Authenticated Post Office Protocol (APOP) nicht.
- **Dedizierter Proxy** – Er ermöglicht folgendes:
  - Ausschließliche Verbindungen zu bestimmten POP3-Servern an alternativen Ports.
  - Standardmäßiges Port-Aliasing an einen einzelnen POP3-Server.
  - Bestimmte Port-Verbindungen zu APOP-Authentifizierungsservern.

Generischer Proxy

Wenn über das Gerät eine generische Proxy-Verbindung hergestellt wird, trennt das Gerät den Benutzernamen, den Hostnamen und die Port-Nummer durch die Begrenzungszeichen Raute (#) und Doppelpunkt (:), wie im folgenden Beispiel:

```
Benutzer#Host:Port
```

Sie können auch andere Begrenzungszeichen festlegen.

HINWEIS: Da Sie Ihr Gerät mit einer Port-Nummer für generische Verbindungen konfigurieren, müssen Ihre POP3-Clients (Software) diese Port-Nummer nicht jedesmal angeben, wenn sie über das Gerät eine generische POP3-Verbindung herstellen.

Dedizierter Proxy

Stellt ein Benutzer über das Gerät eine dedizierte Proxy-Verbindung her, verwendet das Gerät den angegebenen Port, um den POP3-Server zu erreichen. Sie müssen für jeden Server eine eindeutige Port-Nummer angeben. Es wird empfohlen, Zahlen zwischen 1024 und 32767 zu wählen, da die Zahlen bis 1024 in der Regel anderen Protokollen zugewiesen sind. Sie können Verbindungen zu beliebig vielen Servern gestatten.

TIP: Sie können den generischen Port (standardmäßig 110) für eine dedizierte Proxy-Verbindung verwenden. Die dedizierte Verbindung hat Vorrang vor allen generischen Verbindungen.

Weitere Informationen zu POP3 finden Sie in Kapitel 6, Seite 53.

Standardeinstellungen A

In diesem Anhang sind die Standardeinstellungen aufgeführt, über die das Gerät bei der Auslieferung verfügt.

- „Systemeinstellungen“ unten.
- „E-Mail-Einstellungen (SMTP)“ auf Seite 83.
- „Einstellungen für Dateiübertragung (FTP)“ auf Seite 85.
- „Einstellungen für das Surfen im Internet (HTTP)“ auf Seite 85.
- „Einstellungen für Mail-Download (POP3)“ auf Seite 86.
- „Einstellungen für die Virenprüfung“ auf Seite 87.
- „Einstellungen für Protokolle und Warnungen“ auf Seite 88.

Sie können die Einstellungen des Geräts jederzeit auf die Standardwerte zurücksetzen, indem Sie die Gerätesoftware wiederherstellen. Informationen hierzu finden Sie im Installationshandbuch. Dies wird unter Umständen erforderlich, wenn Sie das Gerät in einem anderen Bereich Ihres Unternehmens verwenden möchten.

Systemeinstellungen

Eigenschaft	Wert
WebShield e250:	
• Benutzername	e250
• Kennwort	e250changeme
• Gerätename (Hostname)	webshielde250
WebShield e500:	
• Benutzername	e500
• Kennwort	e500changeme
• Gerätename (Hostname)	webshielde500
DNS-Server	[leer]
Domänenname	.Beispiel
Standard-Gateway	[leer]

Eigenschaft	Wert
Aktivierte Protokolle:	
• E-Mail (SMTP)	JA
• Dateiübertragung (FTP)	JA
• Surfen im Internet (HTTP)	JA
• Mail-Download (POP3)	JA
Transparenz aktivieren	NEIN
Systemsprache	Englisch
IP-Adresse von LAN 1:	10.1.1.108
Subnet-Maske	255.255.255.0
Netzwerkadresse deaktivieren	NEIN
IP-Adresse von LAN 2:	10.1.2.108
Subnet-Maske	255.255.255.0
Netzwerkadresse deaktivieren	NEIN
LAN 2 deaktivieren	NEIN
Interne Netzwerke	[leer]
Externe Netzwerke	Domäne * [alle]
Statische Routen	[leer]
Dynamisches Routing aktivieren	NEIN
Systemprofil	Vom Benutzer ausgewählte Werte der Konfigurationsseiten für die verschiedenen Protokolle
Aufbewahrungszeitraum der Systemprotokolle	23 Tage

E-Mail-Einstellungen (SMTP)

Eigenschaft	Wert
E-Mail-Adresse des Postmasters	[leer]
Anti-Relay für E-Mail-Nachrichten	[leer]
Anti-Spam bei E-Mail-Nachrichten	[leer]
Verwendete Zustellmethoden für E-Mail: • Lokale Domänen • DNS • Ersatz-Relays	 JA JA JA
Lokale Domänen	[leer]
Ersatz-Relays	[leer]
Inhaltsüberwachung bei E-Mail-Nachrichten	NEIN [keine Regeln eingegeben]
E-Mail-Quarantäne	[leer]
E-Mail-Anlagen *(Ein- und ausgehende Nachrichten haben dieselben Einstellungen.)*	
Vorgehensweise für Anlagen von Nachrichten	Alle Anlagen zulassen
Nachrichten sperren, die größer sind als	0 KB [deaktiviert]
Vorgehensweise für geänderte Nachrichten (wenn die infizierten Anhänge entfernt sind)	An Absender zurücksenden, und zwar über die E-Mail-Adresse des Postmasters
Der Nachricht Warnungstext hinzufügen	JA

Eigenschaft	Wert
Warnungstext	<html><head><meta HTTP-EQUIV=”Content-Type” content=”text/html; charset=”> <title>VIRUSINFEKTIONSWARNUNG</title></head> <body> VIRUSINFEKTIONSWARNUNG Das WebShield&reg-Gerät hat in dieser Datei einen Virus entdeckt. Die Datei wurde nicht gesäubert und wurde entfernt. Weitere Informationen erhalten Sie von Ihrem Systemadministrator. Dateiname: %f Virusname: %v Copyright © 1993-2001, Networks Associates Technology, Inc. Alle Rechte vorbehalten. http://www.mcafeeb2b.com </body></html>
Erläuterungstext für eingehende Nachrichten	NEIN
Erläuterungstext für ausgehende Nachrichten	NEIN
E-Mail-Konfiguration	
Eingehende Nachrichten scannen	JA
Ausgehende Nachrichten scannen	JA
Port, an dem E-Mail-Nachrichten empfangen werden	25
Anfängliche Anzahl Listener	35
Anzahl Verbindungen pro Listener	1
Speicherkapazität für Virenprüfung pro Verbindung	4000 KB

Eigenschaft	Wert
Eingehende Nachricht	NEIN
Ausgehende Nachricht	NEIN

Einstellungen für Dateiübertragung (FTP)

Eigenschaft	Wert
Eingehende Nachrichten scannen	JA
Ausgehende Nachrichten scannen	JA
8-Bit-Datenübertragung im ASCII-Modus sperren	JA
Port, an dem Daten empfangen werden	21
Anfängliche Anzahl Listener	1
Anzahl Verbindungen pro Listener	25
Speicherkapazität für Virenprüfung pro Verbindung	4000 KB
Eingehende Nachricht:	
• Begrüßung	NEIN
• Übergabe-Host	[leer]
Ausgehende Nachricht:	
• Begrüßung	NEIN
• Übergabe-Host	[leer]

Einstellungen für das Surfen im Internet (HTTP)

Eigenschaft	Wert
Sperren von Inhalt beim Surfen im Internet	
Zu sperrender Inhalt:	
• ActiveX-Komponenten	NEIN
• Java-Applets	NEIN
• Skript-Sprachen	NEIN
Zu sperrende URL-Teilstrings	[leer]

Eigenschaft	Wert
Konfiguration für das Surfen im Internet	
Eingehende Nachrichten scannen	JA
Ausgehende Nachrichten scannen	JA
Port, an dem Daten empfangen werden	80
Anfängliche Anzahl Listener	1
Anzahl Verbindungen pro Listener	250
Speicherkapazität für Virenprüfung pro Verbindung	4000 KB
Eingehende Nachrichten:	
• Stream-Medien zulassen	NEIN
• Übergabe-Host	[leer]
Ausgehende Nachrichten:	
• Stream-Medien zulassen	NEIN
• Übergabe-Host	[leer]

Einstellungen für Mail-Download (POP3)

Eigenschaft	Wert
POP3-Verkehr scannen	JA
Anfängliche Anzahl Listener	1
Anzahl Verbindungen pro Listener	25
Speicherkapazität für Virenprüfung pro Verbindung	4000 KB
Generische Verbindungen:	
• Port, an dem empfangen werden soll	110
• Begrenzungszeichen	[Benutzer] # [Host] : [Port]
Dedizierte Verbindungen	[leer]
Ersatznachricht	POP3 kann diese Nachricht nicht abrufen.

Einstellungen für die Virenprüfung

Eigenschaft	Wert
Virenprüfung *(Ein- und ausgehende Nachrichten haben dieselben Einstellungen.)*	
Scan-Ebene	Hoch – Höchste Sicherheit. Alle Dateien, einschließlich der komprimierten Dateien, werden gescannt.
Nach unbekannten Makroviren suchen	NEIN
Nach unbekannten Programmviren suchen	NEIN
Aktion, die bei Entdecken einer infizierten Datei ausgeführt werden soll	Bereinigen
Irreparable Dateien in Quarantänebereich verschieben	JA
Automatische Aktualisierung der Antiviren-Software	
Servername der FTP-Site	ftp.nai.com
Pfad zu DAT-/Moduldateien	/virusdefs/4.x
Server-Benutzername	anonym
Kennwort	[maskiert]
Proxy-Server	[leer]
Port-Nummer des Proxy	[leer]
Proxy-Benutzername	[leer]
Proxy-Kennwort	[leer]
DAT-Aktualisierungszeitplan	Donnerstag
Zeitplan für Modul-Aktualisierung	Donnerstag
Uhrzeit	0:0 [12:00]

Einstellungen für Protokolle und Warnungen

Eigenschaft	Wert
E-Mail-Warnungen	NEIN
Verwaltungswarnungen (SNMP)	NEIN
ePolicy Orchestrator-Warnungen	NEIN
Protokollieren	JA
Protokollieren	
Ereignisse des folgenden Typs weiterleiten:	
• Informativ	NEIN
• Erkennung	JA
• Warnung	JA
• Kritisch	JA
• Achtung	JA
Ereignisse für folgende Rollen weiterleiten:	
• Administrator	JA
• Maintainer	JA
• Benutzer	NEIN
Aufbewahrungszeitraum der Protokolle	90 Tage

Index

Symbole

! (Routing-Zeichen), 45
% (Routing-Zeichen), 45

Ziffern

8-Bit-Dateiübertragung, 50

A

Ablenkungen, 62
Active X, 51
Anlagen, 41, 45
Anti-Relay, 43
APOP, 53, 79
ASCII, FTP, 50
Aufsichtsratsvorsitzender, 60
Ausfallsichere Konfiguration, 19, 21, 36
Ausgehende Nachrichten, 10
    getrenntes Scannen, 33
    Virenprüfung, 76
Ausgehendes Szenario
    FTP, 25
    HTTP, 28
    POP3, 30
Authenticated Post Office Protocol (APOP), 79
Auto zu verkaufen, 62

B

Befehlszeilen-FTP-Clients, 24
Begrenzungszeichen, 80
Beispieltopologien, 13
Belästigende E-Mail, 61
Beleidigende Wörter, 61
Bericht, 69
Berlin, Mail-Server, 23
Bidirektionales Scannen, 10
Bitmap, 61
BMP, 46, 61

C

CSV, 69, 71

D

Datenbanken, 46
Dedizierter POP3-Proxy, 53, 80
Diagramm, 69
Direktionale ausfallsichere Konfiguration, 19, 21
Direktionales Scannen, 10
    ausfallsicher, 33
DMZ-Topologie, 22
DNS-Server, 26, 34, 77
Domäne, 75
dos2unix, 50
Drilldown, 70
Drittanbieter
    Software, 46
Dritte
    Weiterleiten an, 43
DTD, 73

E

Echte FTP-Clients, 24
Eingehende Nachrichten, 10
  getrenntes Scannen, 33
  Virenprüfung, 76
Eingehendes Szenario
  FTP, ein Server, 26
  FTP, mehrere Server, 27
  HTTP, 29
  POP3, ein Server, 31
  POP3, mehrere Server, 32
Einkauf, 51
Ein-Standort-Topologie, 15
  mit direktionalem Scannen, 17
Einstellungen, Standard-, 81
E-Mail
  Nachrichten, 77
  Protokollierung, 67
  unerwünschte Nachrichten, 44
ePolicy Orchestrator, 73 bis 74
  Protokollierung, 67
Erhöhen der Fehlertoleranz, 33
Erläuterung, 47
Ersatz-Relays, 77 bis 78
Excel, 69
expliziter Proxy, 13
Externe Netzwerke, 76

F

Fail-Closed-Konfiguration, 36
Fail-Open-Konfiguration, 36
Fail-Over-Konfiguration, 33, 35
Fehlertoleranz, 33
File Transfer Protocol, 79
Firewall, 10, 13, 16
FTP, 10, 49, 76, 79
  ASCII-Modus, 50
  File Transfer Protocol, 49
  Standardeinstellungen, 85
  Szenarios, 24
  Verbindungen über HTTP, 24

G

Generischer POP3-Proxy, 53, 80
Gerät
  Funktionsweise, 10
  Hostname, 74
  Standardeinstellungen, 81
  Verwenden mehrerer Geräte, 33
  Verwendungsweise, 13
Gerät ausschalten, 74
Gerät neu starten, 74
Gesperrte Inhalte, 41
GET-Befehle, 49
Getrenntes Scannen von eingehendem und ausgehendem Datenverkehr, 33
GIF, 46

H

Haftbarkeit, einschränken, 47
Haus zu verkaufen, 62
Hostname, 74
Hot-Fixes, 73
HTTP, 10, 51, 76
  Standardeinstellungen, 85
  Szenarios, 28
Hund, 61

I

Inhaltsüberwachung, 43, 59
Interne Netzwerke, 75
IP-Adresse, 75

J

Java-Applets, 51
Javascript, 51

K

Kanal, 67
Kettenbriefe, 44
Kommagetrennte Dateien, 69
Konfigurationsbeispiele, 13
Kontext, 65

L

Listener, 46, 49, 54
Lokale Domänen, 77
Lotus 123, 69
Lyrik, 44

M

Mail
    herunterladen, 79
    Relays, 77
Mail-Relays, 78
MAPS, 43 bis 44
Mehrere
    Geräte, 33
    Möglichkeiten zur Verwendung des Geräts, 13
Microsoft Excel, 69
Mögliche Netzwerktopologien, 13
MPEGs, 61

N

Nähe, 65
Netzwerk
    Adressen, 75
    Belastung, 61

O

ORBS, 43 bis 44

P

Platzhalter, 64
POP3, 10, 76, 79
    Standardeinstellungen, 86
    Szenarios, 30
Port-Nummer, 46, 49
Post Office Protocol Version 3 (POP3), 79
Postmaster, 42, 68
Professionelles Image, 43
Profil, 77
Projektpläne, 46
ProSiebenSat1.Media AG, 51
Protokolle, 10, 76
    getrenntes Scannen mit mehreren Geräten, 33
Protokollieren
    Standardeinstellungen, 88
Protokollierung
    Details, 68
    Verteilung, 67
Proxies, 10, 39, 76
    dediziert, 53
    generisch, 53
    steuern, 12
Proxymodus, 13
PUT-Befehle, 49

Q

Quarantäne, 74
Bereich bei kritischer Stufe, 68
gesperrte Inhalte, 63

R

Regeln, 59
E-Mail-Weiterleitung, 42
erstellen, 62
Reisen, 51
Relays, 77 bis 78
Routing-Zeichen, 43, 45

S

Scanning profile (Scan-Profil), 77
Schwarze Listen, 44
Servicepacks, 73
SMTP, 10, 41, 76 bis 77
Standardeinstellungen, 83
Szenarios, 15
SNMP-Protokollierung, 67
So werden Sie schnell reich, 62
Spam, 44
Speicherzuordnung, 46, 49, 54
Sport, 51
Standardeinstellungen, 81
Steuern von Proxies, 12
Subnet-Maske, 75
SuperDing, 60
Surfen im Internet, 51
System
Einstellungen, 81
log, 73
Szenarios für die Verwendung, 13

T

Tabellen, 42
Topologie für entmilitarisierte Zone (DMZ), 22
Topologie für internationale Unternehmen, 23
Topologie mit mehreren Standorten, 20
mit direktionalem Scannen, 21
Topologien, in denen das Gerät verwendet werden kann, 13
transparenter Proxy, 13
Transparenzmodus, 13

U

Übergabe-Host, 25
unix2dos, 50
Unterhaltung, 51
Unternehmens-Topologie, 23

V

Verbindungen, 46, 49, 54
Vertrauliche Informationen, 60
Verwenden
Gerät, 13
mehrere Geräte, 33
Viren, 41
scannen, 42
Täuschungen, 44
Virenprüfung, 10, 76
Standardeinstellungen, 87
Virenprüfung, Standardeinstellungen, 87
Visual Basic, 51

W

WAN-Verbindung, 23
Warnungen, 67
    Standardeinstellungen, 88
WebShield-Gerät
    Funktionsweise, 10
    Verwenden mehrerer Geräte, 33
    Verwendungsweise, 13
Weitere Informationen, vii
Weiterleiten, 43
Wide Area Network-Verbindung (WAN)., 23
Wie
    das Gerät funktioniert, 10
    Sie das Gerät verwenden können, 13
Witze, 44

X

XML, 73